

Auszug

16. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für den Zeitraum vom 1. Januar 2019 bis 31. Dezember 2019

1 Einführung

1.1 Entwicklung und Situation des Datenschutzes

Wie ist es um den Stellenwert des Datenschutzes in Sachsen-Anhalt bestellt? Die Bürgerinnen und Bürger und Verbraucherinnen und Verbraucher und Internet-Nutzerinnen und -Nutzer wollen nicht überwacht werden, die Sensibilität für den Wert informationeller Selbstbestimmung ist gewachsen. Die Anzahl der Beschwerden gemäß Datenschutz-Grundverordnung (DS-GVO) steigt weiter. Der Landesbeauftragte profitiert auch von einer verbesserten Zusammenarbeit unter den europäischen Datenschutzaufsichtsbehörden, die europäischen Vorgaben tragen zur Stärkung und Durchsetzungskraft des Datenschutzes bei. Der Staat und seine Behörden bekennen sich zum Datenschutz, doch Regelungswerke und Rechtspraxis zeigen Mängel. Die Wirtschaftsunternehmen sammeln weiter Daten, und nur allmählich wird der Datenschutz als Vertrauens- und Erfolgsfaktor wahrgenommen und umgesetzt. Wirtschaftsverbände und Einzelunternehmen suchen weiter den Rat der Datenschutzbehörde. Und auch die Politik betont gern den Wert eines modernen Datenschutzes.

Diese Einsicht, die zumal die rechtlichen Vorgaben wahrt und sodann die Worte in Taten umsetzt, fehlt auf einem wichtigen Feld allzu sehr: Bei der Personalausstattung der unabhängigen Aufsichtsbehörde wird dieser Anspruch seit Jahren missachtet. Der Landesbeauftragte hat gegenüber dem Landesparlament und der Landesregierung erneut einen Mehrbedarf an Stellen nachdrücklich begründet und angemahnt (s. Nr. 2.2). Dass es infolge der Defizite bei der Personalausstattung zu Defiziten bei der Aufgabenwahrnehmung und damit bei der Durchsetzung des Grundrechtsschutzes kommt, ist selbstkritisch und zugleich als kritische Anfrage an die Politik zu konstatieren.

3 Geschäftsstelle - Fallstatistik

Die Eingänge in der Geschäftsstelle entwickelten sich wie folgt:

2016: 5.506

2017: 6.737

2018: 9.602 (zusätzlich 3.306 Meldungen zu DSB gem. Art. 37 Abs. 7 DS-GVO)

2019: 10.941 (zusätzlich 746 Meldungen zu DSB gem. Art. 37 Abs. 7 DS-GVO)

Im Berichtszeitraum wurden folgende statistische Angaben erfasst:

Beschwerden und Eingaben	437
Informations- und Beratungsfälle (schriftlich wie mündlich)	1051
Vorträge und Veranstaltungen	12
Meldungen von Datenschutzverletzungen	186
Abhilfemaßnahmen/Anordnungen	14
Eingeleitete Bußgeldverfahren (vgl. Nr. 16.2)	16
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz)	8
Förmliche Begleitung von Rechtsetzungsvorhaben	24

Die Zahlen der Beschwerden/Eingaben, aber auch der allgemeinen Beratungsfälle, bewegten sich weiterhin auf einem hohen Niveau. Dies ist der Komplexität der Anwendungsfragen der DS-GVO in der Rechtspraxis geschuldet (vgl. Nr. 2.1).

Viele Beratungen erfolgten nach wie vor ausführlich und unmittelbar am Telefon, insbesondere gegenüber Unternehmen und Behörden. Auf diese Weise gelang es erneut, durch Hinweise auf die geltende Rechtslage und deren Beachtung in der Rechtsanwendung bereits im Vorfeld mögliche Datenschutzverstöße zu vermeiden. Dadurch wurde es weiterhin in vielen Fällen auch nicht nötig, Abhilfemaßnahmen anzuordnen (vgl. Nr. 2.1).

6 Technik und Organisation

6.8 Standpunkte zu Microsoft-Produkten

Windows 10

Insbesondere im Hinblick auf Datenabflüsse personenbezogener Daten in Richtung Microsoft und drohende Bußgelder der Datenschutzaufsichtsbehörden wird immer wieder die Frage gestellt, ob Microsoft Windows 10 als Betriebssystem genutzt werden darf. Verschiedene Untersuchungen und Studien (SiSyPHuS Win10 - Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 des BSI⁶, Datenschutz-Folgenabschätzung im Auftrag der niederländischen Regierung 2018, Prüfbericht⁷ des Bayerischen Landesamts für Datenschutzaufsicht 2017, Aktualisierung in dessen 9. Tätigkeitsbericht 2019⁸, Nr. 3.4) kommen zur Aussage, dass dies möglich wäre. Im Fokus stand dabei jedoch meist die Enterprise-Variante der Software für große Unternehmen. Kleine und mittlere Unternehmen, aber auch kleine Behörden, Kommunen, Unternehmen und Privatleute können oder wollen sich oft nur „normale“ Lizenzen leisten oder die bereits vorinstallierten weinternutzen. Auch ist die Konfiguration für die Abschaltung von Zusatzfunktionen alles andere als selbsterklärend. Teilweise werden die Einstellungen von Microsoft - zumeist nach Aktualisierungen - ohne Not verändert oder zurückgesetzt. Damit wird der technische Laie als Nutzer entmündigt und verliert nach und nach die Kontrolle über seine Daten und Anwendungen.

Der Landesbeauftragte rät allgemein, keine veraltete Software einzusetzen (siehe auch Nr. 6.7). Da Microsoft ein Monopol auf das verwendete Betriebssystem hat und Anwendungen unter alternativen Systemen nicht, nicht mehr oder nur unzureichend funktionieren werden, ist klar, dass das Folgebetriebssystem (die Aktualisierung) in den meisten Fällen wieder aus dem Hause Microsoft kommen wird. Das ist dann wohl ein Windows 10.

Rechtlich ist die Nutzung von Windows 10 umstritten. Es gibt verschiedene Defizite, die Nutzer auch aus datenschutzrechtlicher Sicht von einem Umstieg abhalten (sollten). Die Verträge mit Dienstleistern am anderen Ende der Welt sind nicht allumfassend und transparent dargestellt. Wie soll der Nutzer wissen, was im Betriebssystem verdeckt passiert, wenn er hierüber gar nicht informiert wird? Dienste sind nicht datenschutzkonform voreingestellt und auch sind einmal vorgenommene Einstellungen nicht dauerhaft. Welche Dienste erzeugen welche Übertragungen und wo werden diese deaktiviert? Sind gewünschte Funktionalitäten von einer Deaktivierung eines Dienstes betroffen? Zentrales Manko aber sind unklare, versteckte Datenabflüsse durch die Übertragung von Telemetriedaten zu Microsoft.

Untersuchungen Ende 2019 unter anderem durch das Bayerische Landesamt für Datenschutzaufsicht unter Beteiligung von Vertretern von Microsoft haben ergeben, dass die Übermittlung von Telemetriedaten in der damals aktuellen Enterprise-Version 1909 von Windows 10 durch den Nutzer komplett abgeschaltet werden konnte. Allerdings könnte eine solche Einstellung durch Updates jederzeit wieder zurückgesetzt werden.

Die Abschaltbarkeit der Telemetriedatenübertragung in der Enterprise-Version von Windows 10 ist ein erster Schritt hin zu einem datenschutzgerechten Windows-Betriebssystem. Sie betrifft jedoch in erster Linie große Unternehmen und Behörden mit Volumenlizenzvertrag mit Microsoft. Kleine und mittlere Unternehmen und Privatpersonen bleiben außen vor. Für alle Windows 10-Nutzer in der EU gilt gleichermaßen die DS-GVO; deren Regelungen sind generell einzuhalten.

Der Landesbeauftragte weist darauf hin, dass die Anwender für eine datenschutz-konforme Konfiguration der Rechner verantwortlich bleiben und dies nicht Microsoft überlassen dürfen. Es sei denn, Microsoft sieht die Abschaltung der Telemetriedatenübermittlung standardmäßig im Sinne des Prinzips „Data Protection by Default“ vor.

6.9 Mobiles Arbeiten

Den Landesbeauftragten erreichen regelmäßig Anfragen insbesondere zu Erfordernissen des Datenschutzes bzw. der Datensicherheit beim Mobilen Arbeiten. Werden beim Mobilen Arbeiten, also dem beruflichen Tätigwerden außerhalb der Geschäftsräume, z. B. im Home Office oder auf Dienstreisen, personenbezogene Daten elektronisch verarbeitet, so müssen zusätzliche Schutzmaßnahmen ergriffen werden, um den Zugriff Unbefugter zu verhindern. Mobile Datenträger können praktisch überall mitgeführt werden und unterliegen nicht mehr dem Zugangsschutz der Geschäftsräume. Daher muss einer unbefugten Offenlegung von Daten durch Diebstahl oder Verlust vorgebeugt werden.

Smartphones, Tablets, SD-Karten, USB-Sticks, externe Laufwerke und Laptops enthalten Datenspeicher in Form von Flash-Bausteinen oder magnetischen Festplatten. Werden auf diesen mobilen Speichermedien oder auch auf CDs und DVDs personenbezogene Daten gespeichert, so müssen diese gemäß Art. 5 Abs. 1 lit. f DS-GVO durch geeignete technische und organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust abgesichert werden. Gemäß Art. 32 Abs. 1 lit. a DS-GVO kann dies gegebenenfalls unter anderem durch Verschlüsselung gewährleistet werden. Auch eine sichere Verwahrung an einem unzugänglichen bzw. besonders geschützten Ort wäre als organisatorische Maßnahme denkbar. Um eine effektive Verschlüsselung zu gewährleisten, sind auf verschiedenen mobilen Speichermedien unterschiedliche technische Maßnahmen anwendbar.

Der Landesbeauftragte hat zum Datenträgerschutz eine Handreichung entwickelt, die auch auf seiner Homepage veröffentlicht wurde¹⁰.

6.12 Löschungspflicht und Verjährungsfrist

Immer wieder erreichen den Landesbeauftragten Anfragen zum Thema der Aufbewahrungsbefugnis und -fristen sowie der Löschungs- und der Verjährungsfristen.

Dabei erfolgt häufig der Hinweis auf die Verjährungsregelungen als Begründung für die Aufbewahrung von Unterlagen in Abweichung von dem grundsätzlichen Lösungsgebot (Art. 17 Abs. 1 lit. a DS-GVO). Dem liegt i. d. R. das Missverständnis zugrunde, dass Verjährungsregelungen verbindliche „Fristen“ vorgeben oder zumindest indizieren.

Ziel der Verjährung ist der Rechtsfriede, auf den sich ein Schuldner berufen können soll (Verjährungseinrede), wenn eine gewisse Zeit (i. d. R. 3 Jahre gem. BGB) abgelaufen ist. Dann soll das Interesse des Gläubigers an der Durchsetzung seiner Ansprüche zurücktreten. Für Sonderkonstellationen sind längere Verjährungsfristen vorgesehen. Die Regelungen stellen einen Ausgleich der Interessen des Gläubigers an der Durchsetzung seiner Ansprüche und des Schuldners, nicht nach langer Zeit unerwartet noch in Anspruch genommen zu werden, dar.

Der Regelungshintergrund dieser Ausgleichsregelungen ist ein völlig anderer als der der datenschutzrechtlichen Aufbewahrungs- bzw. Lösungsregelungen:

Bei diesen wird die Speicherung von Daten als Grundrechtseingriff erlaubt, weil notwendige Belange der Allgemeinheit das Schutzinteresse des Betroffenen überwiegen. Zum Teil wird so die Aufbewahrung aus besonderen Gründen für längere Fristen gesetzlich oder berufsrechtlich vorgegeben (Handels- oder Steuerrecht, Berufsordnung der Ärzte). Im Übrigen ist zu prüfen, ob der Verantwortliche die Daten für die Erfüllung seiner Aufgaben bzw. eines bestimmten Zweckes noch benötigt. Ansonsten überwiegt das Lösungsinteresse des Betroffenen (Art. 17 Abs. 1 lit. a DS-GVO). Ist daher eine Aufbewahrung von Informationen nicht mehr geboten oder aus konkreten Anlässen nicht mehr erforderlich, überwiegt das Schutzinteresse der betroffenen Person mögliche Restinteressen des Verantwortlichen.

Eine über die übliche Bearbeitung eines Vorgangs hinausgehende Aufbewahrung kann also nicht mit Verjährungsfristen gerechtfertigt werden. Sie wäre nur ausnahmsweise zulässig, wenn nach der Art des Vorgangs nach belegbarer Erfahrung damit gerechnet werden muss, dass in einem bestimmten Zeitraum nach der üblichen Bearbeitung in relevanter Größenordnung ein weiterer Verarbeitungsbedarf entsteht. Dies kann beispielsweise für Dokumentationen von konkreten Operationen gelten, bei denen erfahrungsgemäß nach weit über 10 Jahren mit Klagen zu rechnen ist.

7 Telekommunikation und Medien

7.2 Verantwortlichkeit für Fanpages bei Facebook

Ausgehend vom Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hatte die DSK am 6. Juni 2018 eine EntschlieÙung verabschiedet. In dieser wurde darauf hingewiesen, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages hinsichtlich der Informationspflichten gegenüber den Nutzern besteht. Die Fanpagebetreiber können ihre datenschutzrechtliche Verantwortung nur erfüllen, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäÙen Betrieb in Europa ermöglicht.

Da Facebook auch nach dem EuGH-Urteil keine wesentlichen Änderungen in seinem Angebot vorgenommen und insbesondere keine Vereinbarung nach Art. 26 DS-GVO zur Verfügung gestellt hatte, wurde am 5. September 2018 ein Beschluss der DSK veröffentlicht, in dem festgestellt wurde, dass der Betrieb einer Fanpage ohne Vereinbarung nach Art. 26 DS-GVO rechtswidrig ist. Als Bestandteil des Beschlusses wurde ein Fragenkatalog veröffentlicht, dessen Fragen sowohl von Facebook als auch vom Betreiber der Fanpage beantwortet werden müssen (vgl. zur Entwicklung XV. Tätigkeitsbericht, Nr. 6.2).

Möglicherweise als Reaktion auf den Beschluss der DSK veröffentlichte Facebook am 11. September 2018 ein sog. Addendum. Die „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“ erfüllen jedoch nicht die Anforderungen an eine Vereinbarung nach Art. 26 DS-GVO (Seiten-Insights sind Statistiken über die Interaktion von Besucherinnen und Besuchern mit einer Fanpage.). Unter anderem stellen die veröffentlichten Informationen die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen.

Diese Einschätzung wurde Anfang April 2019 durch die DSK in einer „Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit“ veröffentlicht (Anlage 1, Anmerkung: Hier nicht beigelegt). Darin wurde noch einmal bekräftigt, dass sowohl Facebook als auch die Fanpage-Betreiber ihrer Rechenschaftspflicht nachkommen müssen, da ansonsten ein datenschutzkonformer Betrieb von Fanpages nicht möglich ist.

Die Maßgaben aus dem EuGH-Urteil und den Positionspapieren der DSK wurden der Staatskanzlei mit Hinblick auf deren Fanpage bei Facebook erläutert. Wegen durchgreifender rechtlicher Bedenken und haftungsrechtlicher Risiken schaltete die Staatskanzlei die Fanpage zunächst ab, reaktivierte sie jedoch im Zuge der Corona-Pandemie im März 2020.

Der Landesbeauftragte kommentierte auch den Entwurf eines Social-Media-Konzepts der Landespolizei kritisch.

Natürlich gehören die Öffentlichkeitsarbeit und die Versorgung der Bürgerinnen und Bürger mit umfassenden Informationen zu den Aufgaben von Behörden. Allerdings ist die Weitergabe personenbezogener Daten an Facebook oder andere Social Media-Anbieter zur Erfüllung deren eigener kommerzieller Geschäftszwecke im Rahmen der Öffentlichkeitsarbeit nicht erforderlich und kann somit nicht auf Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 4 DSAG LSA gestützt werden.

Ende Oktober 2019 veröffentlichte Facebook eine überarbeitete Version seiner o. g. Dokumente. Diese wurden von einer Unterarbeitsgruppe der DSK rechtlich bewertet. Dabei wurde eine weitere EuGH-Entscheidung miteinbezogen: Am 29. Juli 2019 hat der EuGH in einem Urteil festgestellt, dass Betreiber einer Webseite, in die ein „Gefällt mir“-Button von Facebook eingebunden wird, für die Einhaltung der Datenschutzbestimmungen mitverantwortlich sind (Az. C-40/17; NJW 2019, 2755). Im Ergebnis stellte die Unterarbeitsgruppe fest, dass auch die zusätzlichen Informationen im Addendum nicht hinreichend sind, um auf deren Grundlage bewerten zu können, ob eine rechtskonforme Verarbeitung gemäß einer Rechtsgrundlage aus Art. 6 Abs. 1 DS-GVO möglich ist. Das liegt u. a. daran, dass die Datenverarbeitung für Seiten-Insights nicht vollständig, sondern nur beispielhaft dargelegt wird.

Ergänzend ist noch auf Folgendes aufmerksam zu machen: Durch das Bundesverwaltungsgericht wurde am 11. September 2019 aufgrund des EuGH-Urteils vom 5. Juni 2018 folgerichtig entschieden, dass eine Datenschutzaufsichtsbehörde den Betrieb einer Facebook-Fanpage ermessensfehlerfrei auch gegenüber dem Betreiber untersagen kann, da dieser für die Verarbeitung der Nutzerdaten mitverantwortlich ist (Az. 6 C 15.18; NJW 2020, 414).

Angesichts der aktuellen Rechtslage rät der Landesbeauftragte nach wie vor vom Betrieb einer Facebook-Fanpage ab. Dies gilt nicht nur für Behörden, denen eine besondere Vorbildfunktion zukommt, sondern auch für Unternehmen und Vereine. Der Landesbeauftragte wird seine Beratungen insbesondere gegenüber öffentlichen Stellen fortsetzen und verstärken.

10 Rechtspflege und Justizvollzug

10.2 Elektronischer Rechtsverkehr in der Justiz - Sachstand

Der Landesbeauftragte hatte zuletzt in seinem XV. Tätigkeitsbericht (Nr. 9.3) über die Einführung des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akte (e-Akte) in der Justiz informiert. Im Berichtszeitraum fand nur eine Sitzung des Projektlenkungsausschusses des Ministeriums für Justiz und Gleichstellung am 12. September 2019 statt, an der der Landesbeauftragte als Gast teilgenommen hat.

Beim Betrieb des ERV über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) selbst haben sich die Eingangszahlen bei den zentralen Eingangsstellen der Gerichte im Vergleich zum Vorjahr (auf niedrigem Niveau) verdoppelt.

Die Einführung der e-Akte im Bereich der Justiz verzögert sich weiter. Die e-Akte ist bisher für die Justiz in Sachsen-Anhalt aber nur eine „Einbahnstraße“, denn die Gerichte sind noch nicht in der Lage, die z. B. von Anwaltskanzleien elektronisch übermittelten Akten an alle Beteiligten weiterzuleiten. Deshalb werden in den Gerichten mit hohem Personalaufwand die elektronisch übersandten Akten und Vorgänge noch Seite für Seite ausgedruckt und dann wie in „alten Zeiten“ per Post versandt - von „Elektronischem Rechtsverkehr“ kann man hier nicht sprechen.

Auf Grund des derzeit nicht BSI-konform betriebenen Justizrechenzentrums in Barby sowie der künftig geplanten zentralen Bereitstellung der einzelnen Module der e²-Software-Suite wurde mit dem Aufbau des Backend-Betriebes für die e²-Pilotierung im Rechenzentrum (RZ²) des zentralen IT-Dienstleisters des Landes Dataport Anfang des Jahres 2019 begonnen. Für die Pilotierung der elektronischen Aktenverarbeitung wurde das Sozialgericht Magdeburg ausgewählt.

In Bezug auf das besondere elektronische Behördenpostfach (beBPo) ist mittlerweile der Durchführungserlass veröffentlicht (MBI. LSA 2019, S. 169). Die Einrichtung der Behördenpostfächer hat begonnen.

11 Forschung, Hochschulen und Schulen

11.2 Schulwesen

11.2.1 Digitalpakt Schule

Im XV. Tätigkeitsbericht (Nr. 10.2.2) hatte der Landesbeauftragte das mühsame Zustandekommen des Bund-Länder-Projekts Digitalpakt Schule beschrieben, mit dem bis zu fünf Milliarden Euro in die Verbesserung der technischen Ausstattung der Schulen investiert werden sollten. Nach einer Änderung des Grundgesetzes im Frühjahr 2019 wurde der Grundstein für die gemeinsame Finanzierung durch Bund und Länder gelegt. Nun stehen 137 Millionen Euro für die digitale Infrastruktur der Schulen in Sachsen-Anhalt zur Verfügung (vorrangig Netzwerk im Schulgebäude, daneben Laptops, Tablets, interaktive Tafeln etc.). Voraussetzung der Förderung ist ein breitbandiger Internetanschluss. Nach der Förderleitlinie des Bildungsministeriums zur IT-Ausstattung in Schulen muss zudem ein schlüssiges Medienkonzept der Schule vorgelegt werden (vgl. LT-Drs. 7/4995).

Zur Unterstützung der Schulen und Schulträger wurde im Landesinstitut für Schulqualität und Lehrerbildung eine Beratungsstelle „Landesinitiative für nachhaltige digitale Infrastrukturen für Schule und Unterricht“ (LINDIUS) eingerichtet (vgl. auch LT-Drs. 7/5620). Hierzu gehören auch die medienpädagogischen Berater (vgl. Nr. 11.2.2).

Aus Sicht des Landesbeauftragten ist die digitale Ausstattung zunächst ein wichtiger Schritt. Sie muss aber nicht nur mit einem Medienkonzept verbunden werden, sondern dieses muss insbesondere im Sinne einer breit angelegten Medienbildung in der Unterrichtsgestaltung umgesetzt werden. Es gilt der Grundsatz: Technik folgt der Pädagogik. Es reicht nicht aus, die Schulen technisch auszustatten, ohne begleitend im Sinne eines ganzheitlichen, nachhaltigen und verbindlichen Ansatzes auch die Medienbildungsaspekte einzubeziehen. In der Digitalen Agenda der Landesregierung wird Medienkompetenz als ein Schlüssel zur digitalen Welt beschrieben. Die Schulen sind dabei besonders angesprochen. Zusätzlich werden Datenschutz und Informationssicherheit als Querschnittsthemen gerade in diesem Zusammenhang genannt. Mit dem Lernen mit Technik ist also auch das Lernen über die Technik zu verbinden. Das Konzept des Bildungsministeriums „Bildung in der digitalen Welt durch den Einsatz digitaler Medien und Werkzeuge an den Schulen des Landes Sachsen-Anhalt“ hat diesen Zusammenhang aufgegriffen.

Der Landesbeauftragte betrachtet allerdings den Umfang der finanziellen Förderung mit Sorge, denn die Mittel dürften schon nicht für eine komplette Verkabelung aller Schulgebäude in allen Schulen ausreichen, und ohnehin nicht für die Folgekosten für Lizenzen, Wartung, Ablöse von Hard- und Software und zumal für die Fortbildung der Lehrkräfte.

Auch muss die Verarbeitung von teils sensiblen Schülerdaten bei der Nutzung digitaler Bildungsmedien differenziert im Schulgesetz geregelt werden. Es ist notwendig, dass die Daten in der Hoheit der Schule bleiben und auch die Kommunikation mit den Lehrkräften zentral in der Hand des Landes verwaltet wird.

11.2.4 Schul-Cloud des Hasso-Plattner-Instituts

Das Hasso-Plattner-Institut (HPI) in Potsdam entwickelt mit Bundesförderung eine Schul-Cloud. Die Schul-Cloud ermöglicht die Einbindung digitaler Lerninhalte und den Zugriff darauf sowie die Kommunikation mittels Tablet oder Smartphone. Die Datenschutzaufsichtsbehörden des Bundes und der Länder beraten das HPI in datenschutzrechtlicher Hinsicht. Die Rechtsgrundlage ist zunächst die Einwilligung der Betroffenen. Die Datenschutzaufsichtsbehörden haben aber empfohlen, eine verbindliche Nutzung auf gesetzlicher Grundlage auszugestalten. Die Beratung bezieht sich auf die Inhalte des Datenschutzkonzeptes, die vorgesehene Pseudonymisierung von Schülerdaten, die vertragliche Ausgestaltung der Beziehung zwischen Schule und HPI, die Einbindung von Inhaltsanbietern und weitere Detailfragen. Der Landesbeauftragte war in einer Unterarbeitsgruppe des Arbeitskreises Schulen und Bildungseinrichtungen der DSK an den Beratungen beteiligt. Der eigentliche Praxistest, zumal im Hinblick auf die Datensicherheit der Schul-Cloud, steht aus.

11.2.5 Messengerdienste in Schulen

Ausdrückliche Handlungsempfehlungen zu Messengerdiensten an Schulen in Sachsen-Anhalt gab es im Berichtszeitraum nicht. Auch die Handreichung „Datenschutz an Schulen“ des Ministeriums für Bildung des Landes Sachsen-Anhalt, die vielfältige Hinweise zur Datenverarbeitung im Schulkontext auch in Bezug auf technische Belange gibt, verhält sich hierzu nicht. Einschränkende Vorgaben finden sich darin aber zu der mit der Verwendung von Messengerdiensten oft verbundenen Nutzung von privaten Geräten für schulische Zwecke. Ergänzend sind die Hinweise des Bildungsministeriums in der Bekanntmachung vom 19. November 2014 (SVBl. LSA Nr. 1/2015, S. 8) zum Umgang mit sozialen Netzwerken in den Schulen zu berücksichtigen, die sich ebenfalls gegen die Nutzung derartiger Dienste für dienstliche oder personenbezogene Informationen aussprechen.

Die Verarbeitung von Daten von Schülerinnen und Schülern, aber auch von Eltern, unter Einsatz von Messengerdiensten begegnet grundsätzlichen datenschutzrechtlichen Bedenken. Dies gilt nicht, soweit Messengerdienste im Unterricht mit schulischen Geräten unter Anleitung von Lehrkräften im Rahmen der Medienbildung zu Demonstrationszwecken verwendet werden. Dabei darf aber niemand gezwungen werden, sich persönlich bei einem Dienst anzumelden.

Datenverarbeitungen durch die Schule und somit auch durch die Lehrkräfte der Schule zur Kommunikation und zur Bearbeitung von Unterrichtsgegenständen sind inhaltlich nur im Rahmen des § 84a Schulgesetz zulässig. Eine ggf. mit der Nutzung derartiger Dienste verbundene Offenbarung von unterrichts- oder notenrelevanten Daten an Unbefugte ist grundsätzlich unzulässig. Weiter ist auch die Erforderlichkeit und damit die Unerlässlichkeit der Nutzung eines Messengerdienstes für schulische Zwecke fraglich.

Alternativ käme die Verarbeitung von Schüler- oder Elterndaten durch die Schule auf Basis einer Einwilligung in Betracht. Auch dies erscheint jedoch problematisch. Zunächst besteht die Gefahr, dass die Kommunikation zu schulisch notwendigen Zwecken nicht mehr möglich ist, wenn seitens der Schüler oder Eltern vom Recht auf jederzeitigen Widerruf der Einwilligung Gebrauch gemacht wird. Zudem bestünden an der nach der Datenschutz-Grundverordnung gebotenen Freiwilligkeit der Einwilligung Zweifel, wenn die vollumfängliche Teilhabe am Unterrichtsgeschehen von der Nutzung eines Messengerdienstes abhinge.

Weiterhin sind die hohen Anforderungen an den Schutz von Daten von Kindern (s. Art. 6 Abs. 1 lit. f, Art. 8 DS-GVO) und an die Vertraulichkeit sowie die hierzu gebotenen technischen und organisatorischen Datenschutzmaßnahmen zu berücksichtigen (s. Art. 5 Abs. 1 lit. f, Art. 32 DS-GVO). Eine ggf. für die Verarbeitung von Schülerdaten vorgesehene Anwendung bedürfte einer detaillierten Prüfung durch den Verantwortlichen, ob die gesetzlichen und insbesondere technischen und organisatorischen Voraussetzungen erfüllt sind. Dies dürfte mit den in der Regel in Schulen vorhandenen Mitteln kaum zu gewährleisten sein. Eine Prüfung der jeweils im Einzelfall genutzten Produkte, insbesondere in ihrer jeweiligen Konfiguration, ist dem Landesbeauftragten aus Kapazitätsgründen nicht möglich.

11.2.7 Einwilligung Minderjähriger

Insbesondere aus dem schulischen Bereich wird der Landesbeauftragte oft gefragt, ob bzw. ab wann Minderjährige selbst in Datenverarbeitungen einwilligen können. Für die datenschutzrechtliche Einwilligungsfähigkeit Minderjähriger gibt es keine klare gesetzliche Regelung, wie etwa die Regelung zur Volljährigkeit. Bei der Einwilligung in Datenverarbeitungen geht es nicht um eine rechtsgeschäftliche Erklärung, die Geschäftsfähigkeit voraussetzt, sondern um die Ausübung des allgemeinen Persönlichkeitsrechts in Gestalt des Rechts auf informationelle Selbstbestimmung.

Minderjährige, die die erforderliche Einsichtsfähigkeit haben, sind selbst befugt, eine datenschutzrechtliche Einwilligung zu erklären. Die Einsichtsfähigkeit beschreibt die hinreichende geistige Entwicklung, die eine sachorientierte, selbstbestimmte Willensbildung aufgrund der Erfassung des Sachverhalts und der möglichen Folgen der Entscheidung ermöglicht. Hiervon ist in der Regel ab einem Alter von 16 Jahren auszugehen, wofür auch die Regelung in Art. 8 Abs. 1 DS-GVO spricht. Es verbleibt aber bei der Notwendigkeit der Bewertung im Einzelfall. Es ist darüber hinaus zumeist empfehlenswert, Minderjährige zumindest ab einem Alter von 14 Jahren zu befragen und bei mangelnder Zustimmung auf die Verarbeitung zu verzichten.

13 Statistik, Kommunales

13.2 Beratungspraxis für Kommunen: Einbindung der Datenschutzbeauftragten

Seit Anwendungsbeginn der DS-GVO haben die Anfragen von Mitarbeitern von Kommunen und von Eigenbetrieben oder Zweckverbänden zugenommen. In vielen Fällen erreichen den Landesbeauftragten per E-Mail Schilderungen eines kurzen Sachverhaltes mit der Bitte um eine datenschutzrechtliche Bewertung oder mit der Bitte, dem Anfragenden zu sagen, wie Verfahren datenschutzgerecht umgesetzt werden können. Dies betrifft z. B. den Fall, dass durch eine Videokamera ein Gebäude oder ein Marktplatz oder ein Denkmal einer Stadt vor ständiger Beschmutzung oder Zerstörung geschützt werden soll oder die Einführung neuer

Technik zur Datenerhebung in einer Stadt oder in deren Eigenbetrieb für die Berechnung von Gebühren.

Der Landesbeauftragte hat in erster Linie die Aufgaben gemäß Art. 57 DS-GVO zu erfüllen. Hierunter fällt z. B. die Überwachung der Einhaltung der DS-GVO, die Sensibilisierung der Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten, die Befassung mit und Aufklärung von Beschwerden von Betroffenen, die Zusammenarbeit mit anderen Aufsichtsbehörden, die Begleitung von Gesetzesvorhaben und vieles mehr.

Der Landesbeauftragte ist auch gegenüber den Kommunen gefordert, rechtliche Hinweise zur datenschutzgerechten Gestaltung von einzelnen Prozessen zu geben und die Kommunen zu beraten. Oftmals stehen die verantwortlichen Stellen für die Datenverarbeitung, und somit auch die einzelnen Bearbeiter in den Kommunen, vor gleichgelagerten datenschutzrechtlichen Fragen. Aus diesem Grund stellt der Landesbeauftragte, auch in Zusammenarbeit mit anderen Landesbeauftragten, zu zentralen und häufig gestellten Fragen Informationen, Kurzpapiere, Orientierungshilfen etc. auf seiner Homepage zur Verfügung.

Jede Kommune und jede andere öffentliche Stelle hat gem. Art. 37 DS-GVO einen Datenschutzbeauftragten zu bestellen. Dieser Datenschutzbeauftragte ist auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, zu benennen. Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DS-GVO näher benannt und diese umfassen auch die Beratung der verantwortlichen Stelle und die Beratung der Beschäftigten hinsichtlich ihrer Pflichten im Umgang mit personenbezogenen Daten. Auch die Zusammenarbeit mit der Aufsichtsbehörde zählt zu seinen Aufgaben.

Vor diesem Hintergrund ist stets vor der Anfrage an den Landesbeauftragten die Stellungnahme des Datenschutzbeauftragten der Kommune oder des Eigenbetriebes oder Zweckverbandes einzuholen und in die eigene vorläufige Bewertung einzubeziehen. Der behördliche Datenschutzbeauftragte kennt die lokalen Gegebenheiten und es wird umständlicher und zeitlich intensiver Schriftverkehr vermieden. Viele Fragen können auch vom behördlichen Datenschutzbeauftragten vor Ort zeitnah beantwortet werden und müssen dann nicht mehr an den Landesbeauftragten weitergeleitet werden.

15 Videoüberwachung

15.2 Videoüberwachung auf Baustellen

Der Landesbeauftragte war im Berichtszeitraum wiederholt mit der Videoüberwachung auf Baustellen befasst. Diese wird oft im Wege der Auftragsverarbeitung (Art. 4 Nr. 8 und Art. 28 DS-GVO) durch ein Sicherheitsunternehmen als Auftragnehmer durchgeführt. Für die Rechtmäßigkeit der Verarbeitung und die Einhaltung der damit einhergehenden Pflichten (z. B. Informationspflichten nach Art. 13 DS-GVO, insbesondere Hinweisschilder am überwachten Bereich) bleibt jedoch auch in diesen Fällen der Auftraggeber (z. B. Bauunternehmer) verantwortlich. Er ist deshalb verpflichtet, gemäß Art. 58 Abs. 1 lit. a DS-GVO der Aufsichtsbehörde die Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Dies bereitete in Einzelfällen Probleme, da die Auftraggeber den Landesbeauftragten lediglich auf den Auftragsverarbeiter verwiesen.

Als Zwecke für die Videoüberwachung auf Baustellen wurde die Aufklärung von Diebstählen, Einbrüchen und Vandalismus angegeben. Diese Zwecke stellen grundsätzlich berechnigte Interessen im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO dar, ebenso wie z. B. die Feststellung von unberechnigtem Betreten während der Nachtzeit. Allerdings ist die Videoüberwachung nur insoweit zulässig, als sie zur Zweckerreichung erforderlich ist, sofern nicht Interessen oder Grundrechte und Grundfreiheiten betroffener Personen überwiegen.

Daraus folgt, dass sich der Erfassungsbereich der Kameras auf die Bereiche beschränken muss, in denen mit Diebstählen, Einbrüchen, Vandalismus oder unberechnigtem Betreten zu rechnen ist. Regelmäßig reicht die Überwachung von Teilen der Baustelle. Die Überwachung unmittelbar angrenzender Bereiche kommt ausnahmsweise nur dann in Betracht, wenn die Überwachung auf der Baustelle zur Zweckerreichung nicht ausreichend geeignet ist. Die Videoüberwachung ist darüber hinaus regelmäßig in zeitlicher Hinsicht zu beschränken. Die genannten Gefahren drohen üblicherweise außerhalb der Zeiten, in denen auf der Baustelle gearbeitet wird. In diesen Fällen ist die Videoüberwachung auf den Zeitraum außerhalb der Arbeitszeiten zu beschränken, um auf diese Weise auch dem Beschäftigtendatenschutz gerecht zu werden.

Da sich die Beschäftigten aufgrund ihrer arbeitsvertraglichen Verpflichtungen der Überwachung häufig nicht entziehen können, ist die Videoüberwachung von Beschäftigten generell besonders problematisch. Dies gilt vor allem dort, wo die Beschäftigten der Videoüberwachung nicht nur flüchtig oder vorübergehend ausgesetzt sind, sondern unmittelbar an einem Dauerarbeitsplatz. Nach der ständigen Rechtsprechung des Bundesarbeitsgerichtes ist daher bei der Überwachung von Beschäftigten ein besonders strenger Maßstab anzusetzen. Einer dauerhaften Mitarbeiterüberwachung müssen äußerst gewichtige berechnigte Interessen des Arbeitgebers gegenüberstehen.

Soll die Videoüberwachung aber dazu dienen, das Personal vom Diebstahl abzuhalten bzw. des Diebstahls zu überführen, ist dies ausschließlich in den engen Grenzen des § 26 Abs. 1 Satz 2 BDSG zulässig. Diese Vorschrift ermöglicht ausschließlich bei einem konkreten Verdacht, der sich mit milderer Mitteln nicht aufklären lässt, die zeitlich und räumlich sehr eng auf die Aufklärung dieses Verdachtes ausgerichtete Videoüberwachung. Eine präventive, dauerhafte Verhaltens- und Leistungskontrolle ist nicht zulässig.

15.4 Videoüberwachung an Schulen

Die Videoüberwachung an Schulen war Gegenstand einer Kleinen Anfrage im Landtag von Sachsen-Anhalt. Die Antwort der Landesregierung (LT-Drs. 7/1843), die u. a. eine tabellarische Darstellung zu den im Land stattfindenden Überwachungen enthielt, ließ datenschutzrechtliche Defizite, u. a. zur Rechtsgrundlage, zum Umfang und zur Speicherdauer erahnen. Auch die Prüfungserfahrung des Landesbeauftragten legte nahe, dass die Voraussetzungen für die Einrichtung derartiger Anlagen und die engen Grenzen der Speicherung und Verwendung der Aufnahmen nicht immer hinreichend bewusst sind (vgl. XIII./XIV. Tätigkeitsbericht, Nr. 14.2). Zur Videoüberwachung zum Zweck der Objektsicherung hatte der Landesbeauftragte bereits im XII. Tätigkeitsbericht (Nr. 15.1.1) umfängliche Ausführungen gemacht.

Mit dem Ziel einer möglichst flächendeckenden Beratung der Schulen und Schulträger hat der Landesbeauftragte daher in Zusammenarbeit mit dem Ministerium für Inneres und Sport eine Handreichung „Optisch-elektronische Überwachung an Schulgebäuden“ erarbeitet.²¹ Darin wurden u. a. die engen Voraussetzungen der Rechtsgrundlage im Landesdatenschutzrecht, die Speicherdauer, die Notwendigkeit der Erstellung eines Verzeichnisses der Verarbeitungstätigkeit und der Anbringung von Hinweisschildern dargestellt. Das Bildungsministerium hat diese Handreichung in der Bekanntmachung vom 17. Juni 2019 (SVBl. LSA 2019, S. 120) übernommen.