SACHSEN-ANHALT

XVI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Dieser Text entspricht der Landtagsdrucksache 7/6184

Telefon:	0391 81803-0
Fax:	0391 81803-33
Internet:	https://datenschutz.sachsen-anhalt.de/
E-Mail:	poststelle@lfd.sachsen-anhalt.de
Anschrift:	Postfach 1947, 39009 Magdeburg
Dienstgebäude:	Leiterstraße 9, 39104 Magdeburg

Vorwort

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung wirksam und sie zeigt positive Wirkung. Der Bericht 2019 behandelt in seinen Schwerpunkten die Anwendungspraxis der Datenschutz-Grundverordnung bei Behörden und Unternehmen in Sachsen-Anhalt und gibt Hinweise für die verantwortlichen datenverarbeitenden Stellen und für die in ihren Grundrechten betroffenen Personen. Daneben werden Vorgänge im Anwendungsbereich der JI-Richtlinie kommentiert. Auch werden Entwicklungen in der Gesetzgebung auf Landes- und Bundesebene sowie bei der Gestaltung der Digitalisierung in Wirtschaft und Gesellschaft beschrieben.

Der Bericht ist Mittel der Öffentlichkeitsarbeit der Behörde. Auch werden der Landtag, die Landesregierung, der Europäische Datenschutzausschuss und die Europäische Kommission unterrichtet.

Die Schlussphase der Erstellung des Berichts (Redaktionsschluss: 1. April 2020) stand im Schatten der Auswirkungen der Corona-Pandemie, der Dienstbetrieb wurde eingeschränkt, und es waren neue Fragen zu Datenverarbeitungen bei der Bewältigung der Krise zu prüfen. Zu den entsprechenden Vorgängen wird im Rahmen des Folgeberichts informiert.

Bei einer weiter unzureichenden Personalausstattung mussten die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle die weiter gestiegenen Beanspruchungen bewältigen. Für den großen geleisteten Einsatz danke ich herzlich.

Mit der Parlamentsreform 2020 (GVBl. LSA 2020, S. 64) hat der Landtag von Sachsen-Anhalt in der Landesverfassung das Quorum für die Wahl des Landesbeauftragten für den Datenschutz von der 2/3-Mehrheit der anwesenden Abgeordneten allein auf die Mehrheit der Mitglieder abgesenkt. Damit sollte die Wahl meines Nachfolgers erleichtert sein. Im Zuge der Reform wurden mit Änderungen im Datenschutz-Grundverordnungs-Ausfüllungsgesetz auch die Amtszeit auf zukünftig fünf Jahre verkürzt und die Möglichkeit einer Abwahl eingeführt. Dies sollte nicht abschreckend wirken für Amtsbewerber.

Ich übe das Amt über das Ende meiner zweiten Amtszeit im März 2017 seither mit allen Rechten und Pflichten weiter aus. Die Jahre im und für den Datenschutz sind erfüllend und herausfordernd gewesen. Dem Datenschutz in Sachsen-Anhalt wünsche ich eine stärkere Anerkennung durch die Politik.

Magdeburg, den 25. Mai 2020

Dr. Harald von Bose
Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

Anlagenverzeichnis

Abkürzungsverzeichnis

A

AK	Arbeitskreis
Art.	Artikel
a. a. O.	am angegebenen Ort

B

BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
beBPo	besonderes elektronisches Behördenpostfach
BfH	Beauftragter für den Haushalt
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BIM	Building Information Modeling
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMG	Bundesmeldegesetz
BMS-LSA	Bildungsmanagementsystem Sachsen-Anhalt
BR	Bundesrat
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BZRG	Bundeszentralregistergesetz

C

CERT	Computer Emergency Response Team
CON.2	Datenschutz-Baustein aus dem IT-Grundschutz-Kompendium

D

DAkkS	Deutsche Akkreditierungsstelle GmbH
DEK	Datenethikkommission
DIN	Deutsches Institut für Normung
DKIM	DomainKeys Identified Mail (Methode der E-Mail-Authentifizierung)
DMARC	Domain-based Message Authentication, Reporting and Conformance (DNS-Eintrag zur SPAM-Abwehr)
DNS	Domain Name System
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA)
DSAnpUG-EU	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie

	(EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)
2. DSAnpUG-EU	Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – 2. DSAnpUG-EU)
DSB	Datenschutzbeauftragter
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DSUG LSA	Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes (Datenschutzrichtlinienumsetzungsgesetz – DSUG LSA)
DS-GVO, DSGVO	Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
DVG	Digitale-Versorgung-Gesetz

E

EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EDPB	European Data Protection Board (dt.: Europäischer Datenschutzausschuss, s. EDSA)
EGovG LSA	Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt – EGovG LSA) vom 24. Juli 2019
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung – Energiewirtschaftsgesetz
ERV	Elektronischer Rechtsverkehr
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
e. V.	eingetragener Verein
E-ZensAG 2021 LSA	Entwurf eines Ausführungsgesetzes des Landes Sachsen-Anhalt zum Zensusgesetz 2021

F

ff.	fortfolgende
FITKO	Föderale IT-Kooperation

G

GDPR	General Data Protection Regulation (dt.: Datenschutz-Grundverordnung, s. DS-GVO)
GG	Grundgesetz
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung

H

HPI	Hasso-Plattner-Institut
HWK	Handwerkskammer

I

IHK	Industrie- und Handelskammer
IHKG	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
ITN-LSA	InformationsTechnischesNetz (Landesnetz) des Landes Sachsen-Anhalt

J

JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

K

Kfz	Kraftfahrzeug
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KoSIT	Koordinierungsstelle für IT-Standards
KunstUrhG	Kunsturhebergesetz

L

LAV	Landesamt für Verbraucherschutz Sachsen-Anhalt
LHO	Landeshaushaltsordnung des Landes Sachsen-Anhalt
LReg.	Landesregierung
LT-Drs.	Landtagsdrucksache

M

MBl.	Ministerialblatt
MII	Medizininformatik-Initiative

N

NKR	Normenkontrollrat

O

OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz

P

PostG	Postgesetz

Q

R

R2	Release 2
RÄStV	Rundfunkänderungsstaatsvertrag
Rn	Randnummer

S

SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SD-Karte	Secure Digital Memory Card
SDM	Standard-Datenschutzmodell
SGB II	Zweites Buch Sozialgesetzbuch
SGB V	Fünftes Buch Sozialgesetzbuch
SGB XII	Zwölftes Buch Sozialgesetzbuch
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SPF	Sender Policy Framework (Eintrag im DNS einer Internet-Domain zur SPAM-Abwehr)
sog.	sogenannte
SQL	Structured Query Language (Datenbanksprache)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StromGVV	Verordnung über Allgemeine Bedingungen für die Grundversorgung von Haushaltskunden und die Ersatzversorgung mit Elektrizität aus dem Niederspannungsnetz – Stromgrundversorgungsverordnung
SiSyPHuS Win10	Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10
SVBl. LSA	Schulverwaltungsblatt Sachsen-Anhalt
s.	siehe

T

TMG	Telemediengesetz

U

USB	Universal Serial Bus
UWG	Gesetz gegen den unlauteren Wettbewerb

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
vgl.	vergleiche
VwVfG	Verwaltungsverfahrensgesetz

W

X

Y

Z

z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZensG 2021	Zensusgesetz 2021
ZensVorbG 2021	Zensusvorbereitungsgesetz 2021

1 Einführung

1.1 Entwicklung und Situation des Datenschutzes

Datenschutz und Informationssicherheit sind Querschnittsthemen und beanspruchen Geltung und Beachtung in allen Lebensgebieten, in Staat, Wirtschaft und Gesellschaft. Digitalisierung gelingt nur mit Datenschutz im Sinne eines grundrechtsorientierten Ansatzes als Schutz vor Gefährdungen des Persönlichkeitsrechts und als Freiheitsmaßstab einer demokratischen Ordnung. Das Aufgaben- und Themenspektrum des Landesbeauftragten und seiner Geschäftsstelle ist immens, die Herausforderungen und Beanspruchungen entsprechend.

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.

Der XIII./XIV. Tätigkeitsbericht (LT-Drs. 7/3361) und der XV. Tätigkeitsbericht (LT-Drs. 7/4095), die einen Zeitraum von fast vier Jahren umfassen, wurden im federführenden Landtagsausschuss für Inneres und Sport sowie in weiteren sieben Fachausschüssen von September 2019 bis Januar 2020 beraten. Hauptgegenstände der zusätzlichen mündlichen Berichterstattungen des Landesbeauftragten, Feststellungen und Empfehlungen betrafen die europäischen und nationalen Rechtsentwicklungen, insbesondere die DS-GVO und deren Ausfüllung sowie Anwendung im Datenalltag, die Beratungs- und Aufsichtspraxis der Behörde des Landesbeauftragten mit Schwerpunkten im Bereich von KMU, Themen des E-Government etwa beim Online-Zugang zu Verwaltungsleistungen, Rechtsfragen zu Fanpages öffentlicher Stellen bei Facebook, Digitalisierungsprojekte in Wirtschaft und Gesellschaft, z. B. im Bereich der Künstlichen Intelligenz, Belange des Gesundheitsdatenschutzes, etwa bei Forschungsprojekten, Technikausstattungen in Schulen und die damit zu verbindende Vermittlung von Medienbildung, und auch Aspekte der Informationssicherheit. Die Landtagsausschüsse nahmen die Ausführungen des Landesbeauftragten im Ergeb-

nis lediglich zur Kenntnis. Zu einer Landtagsdebatte kam es in Abweichung zur bisherigen Praxis nicht.

Viele der vorerwähnten Themen prägen auch diesen XVI. Tätigkeitsbericht. Die Frage nach der datenschutzrechtlichen Begleitung der Digitalisierungsthemen enthält auch strategische Elemente. Der Landesbeauftragte verfolgt hierbei einen ganzheitlichen Ansatz, denn ökonomische Motive allein oder IT-Einsatz allein sind nicht die Treiber einer Digitalisierung der Gesellschaft. Für deren Akzeptanz ist auch ein Grundrechtsverständnis nötig, das im digitalen Wandel den Menschen im Blick behält (vgl. die sog. Frankfurter Erklärung der für Digitalisierung zuständigen Ministerinnen und Minister, Staatssekretärinnen und Staatssekretären und Landesbeauftragten vom 27. September 2019). Hier wird Datenschutz auch zu einem gestaltenden Element, und dies gilt nicht nur für Entwicklungen der Künstlichen Intelligenz. Daneben ist es für ein Agieren von Verwaltung und Wirtschaft auf Augenhöhe dringlich geboten, dass die Verwaltung nachholt und aufholt; eine E-Government-Strategie des Landes mit Datenschutz und Informationssicherheit kann Ganzheitlichkeit und Verbindlichkeit fördern. Auch dies hat der Landesbeauftragte schon seit Jahren gefordert.

1.2 Künstliche Intelligenz

Die Auswertung von Daten mittels Algorithmen und speziell mittels Künstlicher Intelligenz (KI) führt zu vielfältigen Erkenntnissen, neuen Produkten und Dienstleistungen, die neue Möglichkeiten von Wissenschaft und Technologie aufzeigen. Dies gilt etwa für die Bereiche der Medizinforschung, des autonomen Fahrens und der Spracherkennung. Damit verbunden sind auch neue Herausforderungen für den Datenschutz: Seien es Videos, in denen in Echtzeit die Akteure und Inhalte ausgetauscht werden, Verkehrsüberwachungsanlagen, die die Handy-Nutzung am Steuer erfassen, Bücher, die vom PC geschrieben werden oder Bildmanipulationsalgorithmen, die Details aus dem Bild entfernen oder Hintergründe austauschen. Sie alle eint die Dualität von personenbezogenen Daten und darauf operierenden Algorithmen. Aus Beidem entstehen neue Möglichkeiten, aber auch – heute vielfach noch unbekannte – Gefahren. Die Wirtschaft verspricht sich neue Wertschöpfungsmöglichkeiten und ist gewillt, schnellstmöglich konkrete Produkte zu schaffen. Dem wird der Datenschutz nicht im Wege stehen, wenn er denn vom Design an mit ins Boot geholt wird.

Algorithmen der Künstlichen Intelligenz sind für Datenschützer deshalb so interessant, weil die Algorithmen oft auf personenbezogenen Daten operieren und gleichzeitig für den Laien unklar bleibt, wie die Ergebnisse zustande kommen („Black Box“-Prinzip). Es gibt keinen klassischen Algorithmus mehr, der – einmal an die Wand gemalt – alles erklärt und immer zum gleichen, fest einprogrammierten Ergebnis führt, sondern vielfältige Arten von Algorithmen, die miteinander kombiniert und deren Interna zwar erklärt werden, aber von den meisten Menschen nicht mehr verstanden werden können. Hinzu kommt, dass diese Algorithmen keine festen Einstellungen und Handlungsanweisungen mehr enthalten.

Stattdessen werden aus vorhandenen Daten Muster extrahiert und Einstellungen erzeugt (Lernprozess), die Teil des Produkts oder Algorithmus werden, im Verborgenen arbeiten und maßgeblich dafür verantwortlich sind, wie der KI-Algorithmus neue Daten bewertet und zu welchem Ergebnis er letztlich kommt. Sowohl die Rohdaten (das Lernmaterial) als auch die Einstellungen beim Lernprozess und die Interna der

miteinander verwobenen Algorithmen sind relevant. Vielfach werden bei diesem sogenannten „Maschinellen Lernen“ die internen Parameter ständig geändert und an neue Gegebenheiten angepasst. Das System lernt ständig weiter, was dazu führt, dass die Ergebnisse zum Zeitpunkt X anders aussehen können als zum Zeitpunkt Y. Solche Systeme sind bereits bekannt: Wer ein Produkt kaufen möchte, orientiert sich an der Anzahl der guten Bewertungen anderer Kunden oder dem Preis oder dem Hersteller auf einer unabhängigen Webseite und entscheidet sich dann. Neu ist, dass nun nicht mehr nur eine Handvoll, sondern sehr viel mehr Parameter gleichzeitig und parallel ausgewertet werden und der Nutzer nicht weiß, aufgrund welchen Lernmaterials die Gewichtungen verlaufen und damit unklar ist, welcher Parameter den Ausschlag für die Ergebnisliste des Algorithmus gegeben hat. Waren es wirklich der Preis und die gute Qualität, oder überwog z. B. das bisherige Kaufverhalten auf der Webseite, die Rückmeldung der Bank, das Handymodell oder der Wohnort? Niemand kann das im Nachhinein mehr sagen. Aus diesem Grund werden ethische Richtlinien, Transparenzvorgaben und Regelungen benötigt, die durch die Hersteller eingehalten werden müssen.

Die Bundesregierung möchte Deutschland an der Weltspitze der KI-Entwicklung sehen. Ziel sind dabei KI-Systeme, die kompatibel zu den Grundwerten und Freiheitsrechten Deutschlands und der EU sind.

Im September 2018 nahm die von der Bundesregierung eingesetzte unabhängige Datenethikkommission (DEK) ihre Arbeit auf. Sie besteht aus Expertinnen und Experten, die ethische Leitlinien für die Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlagen, Handlungsempfehlungen geben und Regulierungsmöglichkeiten aufzeigen sollen. Ziele sind der Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung des Wohlstands im Informationszeitalter. Im Oktober 2019 hat die DEK ihr Abschlussgutachten an die Bundesregierung übergeben.[1] Beginnend mit allgemeinen ethischen und rechtlichen Grundsätzen und Prinzipien und übergehend zu Anforderungen an den Umgang mit Daten oder Datenrechten und -pflichten gibt die DEK 75 zentrale Handlungsempfehlungen. Diese behandeln unter anderem Bereiche wie Anforderungen an die Nutzung personenbezogener Daten, an algorithmische Systeme oder an den Einsatz von solchen durch staatliche Stellen, aber auch Haftungsfragen.

Parallel dazu laufen die Beratungen der Enquete-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ der 19. Legislaturperiode des Bundestages weiter.

In Sachsen-Anhalt soll die „Digitale Agenda für das Land Sachsen-Anhalt“ (Stand: Dezember 2017) der Landesregierung die Digitalisierung voranbringen. Der Begriff Künstliche Intelligenz findet sich hier noch nicht, jedoch wird erkannt, dass „intelligente Maschinen und Computerprogramme“ immer mehr Aufgaben übernehmen und gefragt, ob dann noch genug für den Menschen übrig bliebe. Immerhin will man sich im Rahmen des 10-Punkte-Plans zum digitalen Wandel für den Datenschutz der Bevölkerung einsetzen. Im August 2019 fand im Rahmen der Digitalen Agenda ein Workshop zum Thema Künstliche Intelligenz in der Leopoldina in Halle (Saale) statt,

[1] https://lsaurl.de/datenethik

an welchem sich der Landesbeauftragte mit einem Vortrag zu „Datenschutz, KI und Ethik" aktiv beteiligte.

Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) verabschiedete im April 2019 eine Entschließung als „Hambacher Erklärung zur Künstlichen Intelligenz“ (**Anlage 3**). In dieser werden die rechtlichen Rahmenbedingungen für den Betrieb von KI-Systemen betrachtet.

Dieser folgte im November die Entschließung „Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen“ (**Anlage 6**), welche mit einem zugehörigen „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“[2] den Verantwortlichen einen Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gibt, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Die Phasen des Lebenszyklus eines KI-Systems werden am Maßstab von Gewährleistungszielen untersucht und aus den rechtlichen Anforderungen werden KI-spezifische technische und organisatorische Maßnahmen abgeleitet und systematisiert.

Das Bundesverfassungsgericht nahm seine Entscheidung zum Grundrechtsausgleich zwischen der Pressefreiheit eines Presseverlags, der seine Berichte in einem Online-Archiv im Internet bereitstellt, und den durch die Berichte Betroffenen im Hinblick auf deren Persönlichkeitsschutz vor Äußerungen in der Öffentlichkeit (sog. Recht auf Vergessen I – Beschluss vom 6. November 2019, 1 BvR 16/13, NJW 2020, 300), im Übrigen zum Anlass, auch das Grundrecht auf informationelle Selbstbestimmung näher zu konturieren. Angesichts der Entwicklungen der Informationstechnologie bei der Nutzung von Algorithmen konstatierte das Gericht, dass dieses Grundrecht intransparenten Verarbeitungsprozessen insbesondere durch private (oftmals marktmächtige) Unternehmen entgegenwirken solle (a.a.O., Rn. 83 bis 92).

Das Zeitalter der KI hat in Deutschland gerade erst begonnen. Es gewinnt insbesondere mit Blick auf den Datenschutz Brisanz. Die von der DSK am 28. Januar 2020 in Berlin durchgeführte Veranstaltung zum Europäischen Datenschutztag behandelte Grundsatzfragen zur Zulässigkeit von KI und einzelne Anwendungsszenarien. Digitalisierung mit Hilfe von KI ist nur zulässig und gelingt auch nur, wenn die Grundrechte dabei beachtet werden. Dies erkennt auch die Europäische Kommission in ihrem Weißbuch zur Künstlichen Intelligenz vom Februar 2020 an. Der Landesbeauftragte wird das Thema sicherlich noch eine lange Zeit kritisch begleiten.

1.3 Digitale Souveränität

Der Begriff „Digitale Souveränität“ wird oft verwandt, wenn es um Aspekte der Sicherheit und Vertrauenswürdigkeit von Informationstechnologien geht.

Aus datenschutzrechtlicher Sicht beinhaltet digitale Souveränität, dass Verantwortliche grundsätzlich *selbst* über Mittel und Wege der Verarbeitung personenbezogener Daten entscheiden sowie Verarbeitungsvorgänge im Wesentlichen nachvollziehen

[2] https://lsaurl.de/popaki

und kontrollieren können. Insofern ist eine Unabhängigkeit von anderen Staaten und globalen Technologieanbietern von besonderer Bedeutung.

Die digitale Souveränität betrifft nicht nur Hard- und Software, sondern auch technische Details wie Schnittstellen, Datenformate und Quellcode bis hin zur Auswahl von Dienstleistern (z. B. bei Rechenzentren, Cloud-Diensten u. ä.). Zwischen diesen Elementen bestehen durch eine zunehmend enge Verknüpfung von Produkten und Dienstleistungen häufig große Abhängigkeiten, so dass z. B. eine Entscheidung für ein bestimmtes Software-System gleichzeitig eine Festlegung auf den zugehörigen Cloud-Dienst des Herstellers sowie die Gerichtsbarkeit an dessen Sitz bedeutet.

Beispielhaft ist hier die Monopolstellung der Firma Microsoft zu nennen, deren Produkte vielfach auch in der Landesverwaltung Sachsen-Anhalt eingesetzt werden und eng miteinander verknüpft sind (z. B. bauen Outlook aus der Microsoft Office Suite, Microsoft Exchange Server und Active Directory ohne offene Schnittstellen aufeinander auf). In Bezug auf die Informationssicherheit bestehen durch den nicht einsehbaren Quellcode von Microsoft-Produkten, wie z. B. bei dem Betriebssystem Windows 10, ebenfalls Unsicherheiten für die Verantwortlichen bezüglich des datenschutzkonformen Einsatzes (s. Nr. 6.8). Der in Windows 10 enthaltene Telemetriedienst übermittelt Metadaten, die auch personenbezogene Daten enthalten, an Microsoft in den USA. Diese Daten können infolge des Cloud-Acts an U.S.-Behörden gelangen. Dabei ist auch der Zugriff von U.S.-Behörden auf Server möglich, die von einem U.S.-Unternehmen kontrolliert werden, sich selbst aber nicht in den USA befinden müssen. Durch die sog. „Cloud-First“-Strategie von Microsoft werden die noch bestehenden lokalen Lösungen (On-Premises) zunehmend durch cloudbasierte Lösungen ersetzt. Mangels der hinreichenden Transparenz über die konkrete Datenverarbeitung besteht deshalb für den Verantwortlichen ein rechtliches Risiko bezüglich der Einhaltung der Datenschutzanforderungen.

Ein aktuelles positives Anwendungsbeispiel: Die Bundesregierung zeigt Interesse daran, den Staat unabhängiger von internationalen Technologieanbietern zu machen, indem sie durch das Bundeswirtschaftsministerium das Projekt Gaia-X initiierte, welches die Realisierung einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Cloudstruktur für Europa anstrebt.

Die digitale Souveränität der Verantwortlichen hat Auswirkungen auf eine wirkungsvolle Umsetzung der DS-GVO: Dies reicht von den Anforderungen des Datenschutzes durch Technikgestaltung über die Gewährleistung von Informationssicherheit und Datenschutzfunktionalitäten bis hin zur Umsetzung der Rechenschaftspflichten. Fehlende digitale Souveränität der datenschutzrechtlich Verantwortlichen (insbesondere des Staates) hat Folgen für die von der Datenverarbeitung Betroffenen, deren individuelle „Datensouveränität“ bzw. informationelle Selbstbestimmung dadurch gefährdet ist.

Hersteller und Anbieter müssen ihre Produkte bzw. Dienstleistungen so gestalten, dass Verantwortliche tatsächlich souverän über deren Einsatz entscheiden und Verarbeitungsvorgänge grundsätzlich kontrollieren können. Verantwortliche müssen ihre digitale Souveränität wieder verstärkt ausüben und mit gezielter Nachfrage nach datenschutzkonformen Produkten und Dienstleistungen auf das Angebot einwirken.

Digitale Souveränität im Hinblick auf Datenschutz erfordert daher unter anderem die Rückgewinnung der Entscheidungsgewalt über den Datenzugriff, über die Konfiguration von Systemen und über die Gestaltung von Prozessen. In einer digitalisierten Welt bedarf es hierfür zunehmend externer Expertise (u. a. auch durch Zertifizierungen), um eine datenschutzrechtliche Prüfung und Kontrolle durchzuführen. Außerdem sollte die Nutzung von Standards angestrebt werden, damit Verantwortliche auch tatsächlich in der Lage sind, Anbieter bei Bedarf wechseln zu können.

Aktuell wird in Gremien des IT-Planungsrates die Stärkung der digitalen Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien diskutiert. Parallel befassen sich eine Mitteilung der Europäischen Kommission mit dem Titel „Gestaltung der digitalen Zukunft Europas“ vom Februar 2020 sowie die Eckpunkte der Bundesregierung für eine Datenstrategie (vom November 2019, Konsultation von Ende Februar bis Anfang April 2020) mit dem Schutz eines Europäischen Binnenmarkts für Daten und einer verbesserten Bereitstellung von (nicht zwingend personenbezogenen) Daten. Der Landesbeauftragte wird über Ergebnisse und weitere Entwicklungen berichten.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die Tätigkeit des Landesbeauftragten bzw. seiner Geschäftsstelle war im Berichtszeitraum weiterhin auch durch Themen und Vorgänge der europäischen Zusammenarbeit geprägt (zu tatsächlichen und rechtlichen Details s. Nrn. 5.1 und 5.2).

Die Tätigkeit des Landesbeauftragten war auf nationaler Ebene in Sachsen-Anhalt im öffentlichen wie nichtöffentlichen Bereich neben einigen Kontrollen und dem Bereitstellen von Informationen insbesondere von Beratungen zum neuen Datenschutzrecht bestimmt.

Die Beratungsaufgaben des Landesbeauftragten sind in der DS-GVO und im BDSG normiert. So sieht Art. 58 Abs. 3 lit. a DS-GVO die Beratung vor, wenn sich Verantwortliche im Rahmen einer Datenschutz-Folgenabschätzung an die Aufsichtsbehörde wenden. Nach Art. 57 Abs. 1 lit. c DS-GVO besteht eine Beratungspflicht nur gegenüber dem Parlament, der Regierung, und anderen Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen. Schließlich benennt § 40 Abs. 6 BDSG die Aufgabe der Beratung gegenüber Datenschutzbeauftragten nichtöffentlicher Stellen.

Gleichwohl sieht es der Landesbeauftragte neben diesen Ansprüchen auf Beratung als seine Aufgabe an, auch darüber hinaus Verantwortliche zu beraten. So können die ihm übertragenen Aufgaben, die Öffentlichkeit aufzuklären und Verantwortliche und Auftragsverarbeiter zu sensibilisieren (vgl. Art. 57 Abs. 1 lit. b und d DS-GVO), schnell in konkrete Beratungen münden. Zudem kann der Landesbeauftragte die wesentlichen Befugnisse nach Art. 58 DS-GVO (z. B. Hinweis, Warnung, Verwarnung, Verbot der Verarbeitung) nur nachvollziehbar wahrnehmen, wenn er seine Auffassung – ähnlich wie in Beratungsfällen – detailliert begründet. Proaktive Beratung und Unterstützung und in der Folge entsprechende Maßnahmen der Verantwortlichen

– ebenfalls proaktiv, und im Falle von schon erfolgten Datenschutzverstößen auch durch Abhilfemaßnahmen – sind allemal besser als repressive Verwaltungs- und Sanktionsverfahren.

Die Anzahl der Informationsanfragen von Unternehmen sowie der Eingaben und Beschwerden, die den Bereich der nichtöffentlichen Verantwortlichen betraf, war in 2019 gegenüber dem letzten Berichtszeitraum nach wie vor auf hohem Niveau. Die Anfragen, Eingaben und Beschwerden hatten zunehmend komplexe und sehr spezielle Datenverarbeitungen zum Inhalt. Dies führt angesichts der begrenzten personellen Ressourcen der Geschäftsstelle des Landesbeauftragten zu verlängerten Bearbeitungszeiten.

Beratungen einzelner Unternehmen fanden zu sehr unterschiedlichen Themen statt, z. B. dem Kundendatenschutz, der Videoüberwachung, der Datenverarbeitung mithilfe von Webshops und der Nutzung von Messengerdiensten. Auch zu Produktentwicklungen wurde beraten, z. B. zu einer Software, die die Datenschutzbeauftragten bei ihrer täglichen Arbeit unterstützen soll. Beschwerden und Meldungen von Datenschutzverletzungen führten zu Kontrollen bei Unternehmen, die in den Fällen, in denen die Gefahr der Beweismittelvernichtung bestand, auch ohne vorherige Ankündigung durchgeführt wurden.

Der Landesbeauftragte hat zwar die Aufgabe, die Öffentlichkeit für die Einhaltung des Datenschutzes zu sensibilisieren und zu informieren, kann diese aber aufgrund der unzureichenden Personalausstattung nur sehr eingeschränkt wahrnehmen. Trotzdem nahmen Vertreter des Landesbeauftragten an unterschiedlichen Arbeitskreisen aus dem Bereich der Wirtschaft teil bzw. gestalteten sie mit. So fand im Frühjahr 2019 eine Beratung mit den Datenschutzbeauftragten der Sparkassen statt, die sich mit deren branchenspezifischen Verarbeitungen befasste. Ferner organisierte die IHK Halle-Dessau mit der HWK Halle einen mehrmals tagenden Arbeitskreis, an dem Vertreter unterschiedlicher Unternehmen teilnahmen. Auch an Veranstaltungen von Datenschutzverbänden, wie der Gesellschaft für Datenschutz und Datensicherheit e. V. und dem Berufsverband der Datenschutzbeauftragten Deutschlands e. V., nahmen Mitarbeiter der Geschäftsstelle des Landesbeauftragten teil und konnten zu vielen Themen die aktuelle Rechtslage darstellen. Auf Einladung des Landesbeauftragten fand wieder ein Treffen mit den für Sachsen-Anhalt zuständigen berufsständischen Kammern statt.

Auf Einladung unterschiedlicher Organisationen hielten der Landesbeauftragte und seine Mitarbeiter Vorträge zu bis dato gemachten Erfahrungen mit der DS-GVO, speziell zum Datenschutz in Vereinen, zum Datenschutz bei KI-Anwendungen (s. Nr. 1.2) und zur vernetzten Planung und Durchführung von Baumaßnahmen (s. Nr. 14.6).

Der Landesbeauftragte nahm weiterhin als beratendes Mitglied an den Sitzungen des Digitalisierungsbeirats zur Digitalen Agenda des Landes teil. Dieses unter der Federführung des Ministeriums für Wirtschaft, Wissenschaft und Digitalisierung eingerichtete Gremium begleitet die Umsetzung der Digitalen Agenda und kommentiert strategische Fragen und Förderprojekte.

Neben der Beratung nichtöffentlicher Stellen gehört die umfängliche Beratung von Behörden seit jeher zu den Hauptaufgaben des Landesbeauftragten (vgl. § 24 Abs. 4

DSAG LSA). Dies betrifft nicht nur die Anwendung der DS-GVO und des allgemeinen Landesdatenschutzrechts, sondern auch die fachspezifischen und fachrechtlichen Fragestellungen sowie die Unterstützung bei Gesetzgebungsvorhaben.

Beispiele für Beratungen aufgrund besonderer Anfragen bzw. Anlässe betrafen das Bildungsmanagementsystem (s. Nr. 11.2.3) und die Problematik des Betreibens von Fanpages durch öffentliche Stellen bei Facebook (s. Nr. 7.2).

Daneben fanden auch weiterhin die langjährig etablierten Gesprächskreise statt. Dies betrifft einmal das Engagement des Landesbeauftragten in der Landesarbeitsgemeinschaft Medienkompetenz. Weiter hatte der Landesbeauftragte zum jährlichen Erfahrungsaustausch mit den Datenschutzbeauftragten der Landkreise und kreisfreien Städte eingeladen und beteiligte sich an der jährlichen Beratung der Hochschuldatenschutzbeauftragten. Auch war der Landesbeauftragte wieder mit einigen Fortbildungen und im Rahmen des Beschäftigtenlehrgangs II für das Aus- und Fortbildungsinstitut des Landes aktiv.

Im Rahmen der Öffentlichkeitsarbeit wurde die Homepage des Landesbeauftragten fortlaufend aktualisiert. So wurden u. a. die Handreichung zur „Optisch-elektronischen Überwachung von Schulgebäuden“ und „Hinweise zum Fotografieren bei Schulveranstaltungen“ auf der Homepage aufgenommen.

2.2 Unzureichende Personalausstattung der Geschäftsstelle

Seit dem 25. Mai 2018 kommt die DS-GVO als neues Datenschutzrecht in der ganzen Europäischen Union zur Anwendung. Mit diesem neuen Recht, das durch neue nationale Regelungen (BDSG, DSG LSA bzw. DSAG LSA) ergänzt wird, sind zahlreiche neue Aufgaben auch für den Landesbeauftragten für den Datenschutz in Sachsen-Anhalt begründet oder ausgeweitet worden. Vor diesem Hintergrund hatten alle Landesbeauftragten für den Datenschutz im Jahre 2016 ein Gutachten hinsichtlich der mit der Gesetzesreform verbundenen Personalbedarfe erstellen lassen. Das von Prof. Roßnagel erstellte Gutachten geht allein aufgrund der Regelungen der DS-GVO von einem zusätzlichen Personalbedarf von 28 Stellen je Aufsichtsbehörde aus (vgl. XIII./XIV. Tätigkeitsbericht, Nr. 2.3).

Ausgehend von einer Personalausstattung von 22 Stellen im Jahr 2016 ist mit dem Anwendungsbeginn der DS-GVO und einem damit verbundenen Zusatzbedarf von 28 Stellen eine Personalausstattung von 50 Stellen erforderlich. Hinzu kommen zwei weitere erforderliche Stellen für die mittlerweile zusätzlich übertragenen Aufgaben „Personal“ und „Haushalt“, einschließlich einer Beauftragten für den Haushalt (BfH) hinsichtlich des Einzelplans 18. Für weitere Aufgaben im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 durch das DSUG LSA und neuer gesetzlicher Kontrollpflichten ist eine weitere Stelle erforderlich, so dass ein Gesamtstellenbedarf von 53 Stellen besteht.

Mit der 2018 vorgenommen Herauslösung der Geschäftsstelle aus dem Bereich des Landtages war die Übernahme der Personalverwaltung und der Haushaltsführung einschließlich der Bestellung einer BfH umzusetzen. Da trotz dieser Übertragung von zwingend abzudeckenden Verwaltungsleistungen keinerlei zusätzliche Stellen bewilligt worden sind, mussten zwei Stellen, die für Datenschutzaufsichtsaufgaben vorgesehen waren, für diese neuen Verwaltungsaufgaben verwendet werden. Die fakti-

sche Kürzung dieser zwei Stellen hat sich auch im Berichtszeitraum insgesamt negativ auf die Aufgabenerfüllung ausgewirkt.

Für den Doppelhaushalt 2017/2018 wurden vom Landtag lediglich vier Stellen bewilligt, für den Haushalt 2019 ebenfalls lediglich vier Stellen (vgl. XV. Tätigkeitsbericht, Nr. 2.2).

Von dem aktuellen Gesamtbedarf von 53 Stellen sind also bislang nur 30 Stellen (einschließlich des Landesbeauftragten) vorhanden, so dass ein offener Stellenbedarf von weiteren 23 Stellen besteht. Um diesen Bedarf stufenweise zu decken, hatte der Landesbeauftragte im Jahre 2019 für die Haushaltsjahre 2020/2021 insgesamt 15 Stellen mit eingehender Begründung im Rahmen der Haushaltsaufstellung angemeldet.

Das Ministerium für Finanzen hat diese Anmeldungen, ohne auf die Begründung der Stellen seitens des Landesbeauftragten einzugehen und ohne die Erforderlichkeit der Stellen zu prüfen, komplett gestrichen. Dadurch wurde dem Landtag im Rahmen des Gesetzentwurfes zum Haushaltsplan/Einzelplan 18 keine der zusätzlichen Stellenanmeldungen vorgelegt. Das Ministerium der Finanzen, das den Landtag stärker in die Haushaltsaufstellung einbinden wollte, folgte auch nicht dem Rechtsgedanken aus den §§ 28, 29 LHO LSA (vgl. Nr. 4.1.1) und unterrichtete den Landtag nicht über den vom Landesbeauftragten geltend gemachten Stellenmehrbedarf.

Der Landesbeauftragte erläuterte in den Haushaltsberatungen im Ausschuss für Finanzen seinen konkreten Stellenbedarf. Gleichwohl bewilligte der Ausschuss für Finanzen bzw. der Landtag dem Landesbeauftragten für seine Geschäftsstelle keinerlei zusätzliche Stelle. Damit setzt sich die defizitäre Personalausstattung der Geschäftsstelle auch in den Jahren 2020 und 2021 fort.

Sowohl die einseitige Streichung ohne Begründung als auch die dabei unterlassene Prüfung der Erforderlichkeit des Stellenbedarfs stellen einen Verstoß gegen europäisches und Landesrecht dar. Art. 52 Abs. 4 DS-GVO, § 21 Abs. 3 Satz 2 DSG LSA bzw. § 22 Abs. 2 Satz 2 DSAG enthalten eine Garantie hinsichtlich der notwendigen Personalausstattung. Die Notwendigkeit der angemeldeten Stellen wurde vom Landesbeauftragten im Rahmen der Haushaltsaufstellung dezidiert begründet. Dieser Bedarf wurde von keinem der am Haushaltsaufstellungsverfahren Beteiligten, weder von der Landesregierung noch vom Landtag, mit Argumenten oder mit Fakten bestritten, sodass die Notwendigkeit der beantragten Stellen nicht wirklich in Frage gestellt werden konnte.

Durch die einseitige Streichung von notwendigen Stellen liegt eine gravierende, unzulässige Einflussnahme in die völlige Unabhängigkeit des Landesbeauftragten vor, die sich sowohl auf die Personalhoheit als auch auf die konkreten Möglichkeiten der Aufgabenbewältigung negativ auswirkt.

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).

4 Nationales und europäisches Datenschutzrecht

4.1 Neue Rechtsgrundlagen im Bundes- und Landesrecht

4.1.1 Anpassung an die Datenschutz-Grundverordnung

Anpassungen im Bundesrecht

Am 25. November 2019 wurde das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. DSAnpUG-EU) verkündet, welches in den wesentlichen Teilen am Tage nach der Verkündung in Kraft getreten ist (BGBl. I 2019, S. 1626). Durch dieses umfangreiche Artikelgesetz werden über 150 Einzelgesetze verändert.

Viele Änderungen beinhalten lediglich die sprachliche Anpassung von Begriffen an die Terminologie der DS-GVO. Zudem wurden Rechtsgrundlagen für die Verarbeitung personenbezogener Daten geschaffen oder justiert. Es wurden Anpassungen zu technischen und organisatorischen Maßnahmen, zur Auftragsverarbeitung, zur Datenübermittlung an Drittländer oder an internationale Organisationen sowie im Bußgeldbereich vorgenommen.

Einige Änderungen wurden auch in dem seit dem 25. Mai 2018 geltenden BDSG vorgenommen, welches ein wesentlicher Teil des 1. DSAnpUG-EU war:

- In § 16 Abs. 4 wurde eine Bestimmung aufgenommen, nach der Aufsichtsbehörden zur Überwachung der Einhaltung der Vorschriften über den Datenschutz bei nichtöffentlichen Stellen das Betreten von Grundstücken und Geschäftsräumen und der Zugang zur Datenverarbeitung nur während der üblichen Betriebs- und Geschäftszeiten zu gewähren ist. Eine vergleichbare Regelung existierte schon in § 38 Abs. 4 des bis zum 25. Mai 2018 geltenden BDSG, wurde aber bisher nicht in das neue BDSG übernommen. Der Landesbeauftragte führte seine Vor-Ort-Kontrollen stets während der Betriebs- und Geschäftszeiten durch.

- Dem § 22 Abs. 1 wurde eine Regelung hinzugefügt, nach der die Verarbeitung von besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) auch für nichtöffentliche Stellen zulässig ist, wenn dies aus Gründen des öffentlichen Interesses zwingend erforderlich ist. Die Vorschrift soll nach der Gesetzesbegründung (BT-Drs. 19/4674, S. 211) Rechtssicherheit schaffen für die nichtöffentlichen Stellen, die sensible Daten mit Sicherheitsrelevanz verarbeiten. Ein solches zwingendes Erfordernis soll etwa bei der Verarbeitung von personenbezogenen Daten mit Religionsbezug durch zivilgesellschaftliche Träger bei Präventions- und Deradikalisierungsprogrammen im Bereich religiös motiviertem, insbesondere islamistischem Extremismus bestehen. Ein erhebliches öffentliches Interesse soll auch bei der Bekämpfung von Pandemien oder im Rahmen des Katastrophenschutzes möglich sein. Der Bundesgesetzgeber beruft sich hinsichtlich seiner Regelungsbefugnis auf Art. 9 Abs. 2 lit. g DS-GVO.

- § 26 Abs. 2 Satz 3 regelt die Form der Einwilligung im Beschäftigtenverhältnis. Die Vorschrift stellt klar, dass eine Einwilligung hier regelmäßig nicht nur schriftlich, sondern auch elektronisch erfolgen kann. Die Vorschriften des BDSG (§ 26 Abs. 2 Satz 1 und 2) und der DS-GVO (Art. 7, ErwGr 32, 42, 43), die ergänzende Regelungen für die Einwilligung im Beschäftigtenverhältnis beinhalten, bleiben unverändert. Danach ist die Einwilligung in Beschäftigtenverhältnissen nach wie vor nur in eng begrenzten Fällen zulässig.

- In § 38 Abs. 1 Satz 1 BDSG wird die Personenanzahl, ab der verpflichtend ein Datenschutzbeauftragter im nichtöffentlichen Bereich zu benennen ist, von 10 auf 20 angehoben. Danach ist ein Datenschutzbeauftragter zu benennen, soweit der Verantwortliche in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Die Vorschrift soll kleine und mittlere Unternehmen sowie Vereine entlasten. Bereits in seinem XV. Tätigkeitsbericht (Nr. 13.2) hat sich der Landesbeauftragte – ähnlich wie die DSK (s. Entschließung vom 23. April 2019, **Anlage 4**) – kritisch zu

der Aufweichung der Voraussetzungen für die Pflicht zur Benennung von Datenschutzbeauftragten geäußert. Zu einer begleitenden Empfehlung des Landesbeauftragten s. Nr. 14.1.

Anpassung des Landesrechts

Im XV. Tätigkeitsbericht (Nr. 4.1.1) hatte der Landesbeauftragte auf das Gesetzesvorhaben zur Anpassung des Landesdatenschutzrechts (LT-Drs. 7/3826) hingewiesen. Artikel 1 dieses Gesetzes ist das Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA).

Das DSAG LSA ersetzt das alte DSG LSA, soweit dieses nicht bereits durch die DS-GVO überlagert worden ist. Zweck des Gesetzes ist die Ergänzung und Beschränkung von Regelungen der DS-GVO. In Ausfüllung der Vorgaben des Art. 6 Abs. 1 lit. e, 2 und 3 und des Art. 23 DS-GVO wird in § 4 DSAG LSA die allgemeine datenschutzrechtliche Rechtsgrundlage für öffentliche Stellen in Sachsen-Anhalt geschaffen. In den §§ 10 ff. werden Beschränkungen der Betroffenenrechte und in den §§ 17 ff. werden Vorschriften für Datenschutzbeauftragte im Anwendungsbereich der JI-Richtlinie geregelt. Schließlich werden die Rechtsstellung, Aufgaben und Befugnisse des Landesbeauftragten als völlig unabhängige Aufsichtsbehörde beschrieben.

Das DSAG LSA ist in den Ausschüssen des Landtages wiederholt und ausführlich beraten worden. Der Landesbeauftragte hatte hierzu Stellung genommen und vorgetragen. Drei Regelungskomplexe sind dabei von besonderer Bedeutung.

Erstens unterblieb die Wiederaufnahme des Landesbeauftragten für den Datenschutz in den Schutz der unabhängigen Geltendmachung von Haushaltsanmeldungen in §§ 28, 29 LHO LSA. Dieser war durch Trennung der Geschäftsstelle des Landesbeauftragten vom Präsidenten des Landtages, der diesen Schutz genießt, entfallen. Das führt im Falle einseitiger Kürzungen oder Streichungen bei der Haushaltsaufstellung zu möglichen Einflussnahmen durch die Landesregierung bzw. das Ministerium der Finanzen. Eine solche Einflussnahme stellt eine europarechtswidrige Beeinträchtigung der Unabhängigkeit dar. Die Unabhängigkeit ist nach der Rechtsprechung des Europäischen Gerichtshofs in einem absoluten Sinn zu verstehen, der jegliche mittelbare oder unmittelbare Einflussnahme von welcher Seite auch immer ausschließe.

Über die auch landesrechtlich vorgegebene, notwendige Personalausstattung des Landesbeauftragten soll der Landesgesetzgeber in Kenntnis der vollständigen Anmeldung des Landesbeauftragten entscheiden können (s. Nr. 2.2). Demgemäß wurde vorgeschlagen, dass die schützenden Verfahrensrechte in § 28 Abs. 3 und § 29 Abs. 3 LHO LSA, die für den Präsidenten des Landtages (und somit bis zum 5. Mai 2018 auch für den Landesbeauftragten) und den Präsidenten des Landesrechnungshofs gelten, auch für den Landesbeauftragten für entsprechend anwendbar erklärt werden.

Der Landtag folgte dem Änderungsvorschlag des Landesbeauftragten im Zusammenhang mit dem DSAG LSA nicht. Der Landesbeauftragte wiederholte daher im Rahmen der Haushaltsanmeldung für 2020/21 sein Anliegen und empfahl eine Er-

gänzung der §§ 28, 29 LHO LSA im Haushaltsbegleitgesetz. Dazu kam es aber nicht.

Zweitens ist die Ausgestaltung der Rechtsdurchsetzung gegenüber öffentlichen Stellen in § 30 DSAG LSA bedenklich. Eine systemkonforme und dem europäischen Anliegen der Stärkung der Datenschutzaufsicht entsprechende Vollstreckbarkeit der Maßnahmen des Landesbeauftragten ist nicht gegeben. Es ist nicht nachvollziehbar, weshalb lediglich in einer Richtung ein Verwaltungsakt fingiert und die Anfechtungsklage von Landesbehörden gegen eventuelle Maßnahmen des Landesbeauftragten zugelassen wird. Im Gegenzug wird aber ein Verwaltungsakt verneint und mangels Vollstreckungsmöglichkeit dem Landesbeauftragten aufgegeben, selbst zu klagen. Der Landesbeauftragte kann also eine unangefochtene Anordnung nicht vollstrecken, sondern muss gegenüber einer Behörde, die seine Anordnung missachtet, auch noch gerichtlich vorgehen. Die vorgesehene gerichtliche Feststellung wäre zudem auch nicht vollstreckbar. Selbst Anordnungen gegenüber Kommunalbehörden, die wohl zweifellos Verwaltungsakte und damit eigentlich vollstreckbar sind, wird die Vollstreckbarkeit „zugunsten“ einer Klage des Landesbeauftragten entzogen. Diese Konstruktion ist schlicht systemfremd und europarechtlich höchst bedenklich.

Drittens ist im parlamentarischen Verfahren die ursprünglich vorgesehene Regelung zur Geltung der DS-GVO und des DSAG LSA für den Landtag geändert worden. Danach entfällt die zunächst vorgesehene Begrenzung der Anwendbarkeit der DS-GVO nur auf Verwaltungstätigkeiten des Landtages. Vielmehr wird, da eine direkte Anwendbarkeit der DS-GVO auf parlamentarische Tätigkeiten nach herrschender Meinung verneint wird, landesgesetzlich die entsprechende Anwendbarkeit der DS-GVO auch auf die gesamte parlamentarische Tätigkeit des Landtages bestimmt. Dem Gesetzeswortlaut sind danach der Landtag, die Fraktionen und die Abgeordneten in ihrer parlamentarischen Tätigkeit grundsätzlich in vollem Umfang den Regelungen der DS-GVO und des DSAG LSA unterworfen. Es gelten damit auch die gesamten Befugnisse der Aufsichtsbehörde nach Art. 58 DS-GVO (u. a. Untersuchungen, Zugang zu allen personenbezogenen Daten und Informationen, Zugang zu den Abgeordnetenbüros, einschließlich aller Datenverarbeitungsanlagen, Anweisungen, vorübergehende oder endgültige Beschränkung der Verarbeitung). Weiter greifen die durch die DS-GVO vorgesehenen Verpflichtungen (Informationspflichten (Art. 13, 14 DS-GVO) und Auskunftspflichten (Art. 15 DS-GVO), Meldung von Datenschutzverstößen, Datenschutz-Folgenabschätzung, etc.).

Jedoch wird mit der Begründung zur Gesetzesänderung versucht, durch Hinweis auf die verfassungskonforme Auslegung (Beachtung des Gewaltenteilungsprinzips) im Rahmen der „entsprechenden“ Anwendung der DS-GVO diese mit dem Wortlaut vorgegebenen Konsequenzen einzuschränken. So soll anstelle der Befugnisse nach Art. 58 DS-GVO lediglich eine „kooperative Beratung“ des Landesbeauftragten zulässig sein. Die Relativierung von Aufsichtsbefugnissen durch Hinweise in den Materialien des Gesetzgebungsverfahrens ist rechtlich unsicher. Die materiellen Verpflichtungen gem. DS-GVO werden durch die Gesetzesbegründung nicht relativiert; denn die Betroffenenrechte haben Grundrechtsqualität. Sie können unter Umständen durch Parlamentsgesetz, nicht aber im Wege der Auslegung des Begriffs „entsprechende Anwendung“ eingeschränkt werden.

Der Landesbeauftragte hatte demgegenüber unter Berücksichtigung des Grundsatzes der Gewaltenteilung empfohlen, wie in fast allen anderen Bundesländern die

Anwendbarkeit der DS-GVO auf die Verwaltungstätigkeiten des Landtags zu beschränken. Dies entspräche auch der bisherigen Rechtspraxis. Eine Statuierung eigener Datenschutzregularien durch den Landtag etwa durch eine Datenschutzordnung hätte sodann verdeutlichen können, dass auch die parlamentarische Tätigkeit keinen rechtsfreien Raum darstellt (vgl. XV. Tätigkeitsbericht, Nr. 4.2 i. V. m. Anlage 4).

Das DSAG LSA ist – ohne dass die o. a. Hinweise des Landesbeauftragten Berücksichtigung fanden – im Rahmen des o. a. Artikelgesetzes am 26. Februar 2020 in Kraft getreten (GVBl. LSA S. 25).

4.1.2 Umsetzung der JI-Richtlinie

Im XV. Tätigkeitsbericht (Nr. 4.1.2) hatte der Landesbeauftragte auf den Gesetzentwurf zur Umsetzung der JI-Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes (LT-Drs. 7/3207) hingewiesen. Bei der Entwurfserstellung hatte er das federführende Ministerium für Inneres und Sport beraten und eine Stellungnahme gegenüber dem Landtag abgegeben. Das Gesetz ist am 10. August 2019 in Kraft getreten (GVBl. LSA S. 218).

Maßgeblicher Teil dieses Artikelgesetzes ist das neue Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt (DSUG LSA) mit Regelungen zur Datenverarbeitung von Behörden bei der Straftatenverhütung und -verfolgung, einschließlich damit in Zusammenhang stehender Gefahrenabwehrmaßnahmen, der Strafvollstreckung und der Verfolgung von Ordnungswidrigkeiten.

Auf Bundesebene ist das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 am 26. November 2019 in Kraft getreten (BGBl. I 2019, S. 1724). Mit ihm wurden im Justizbereich u. a. die Strafprozessordnung, das Strafvollzugsgesetz, die Zivilprozessordnung und diverse Registergesetze an die Vorgaben der Richtlinie und der Datenschutz-Grundverordnung angepasst.

4.2 Evaluierung der DS-GVO

Art. 97 DS-GVO verpflichtet die EU-Kommission, bis spätestens 25. Mai 2020 einen ersten frühen Evaluierungsbericht zur Bewertung und Überprüfung der DS-GVO dem Europäischen Parlament und dem Rat vorzulegen; der Bericht soll veröffentlicht werden. Zur Vorbereitung dieses Berichts übersandte die EU-Kommission im November 2019 den Aufsichtsbehörden der Mitgliedstaaten über den Europäischen Datenschutzausschuss (EDSA) einen Fragenkatalog, der entsprechend Art. 97 Abs. 2 DS-GVO im Wesentlichen die Erfahrungen mit den Kapiteln „V. Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“ und „VII. Zusammenarbeit und Kohärenz“ der DS-GVO abfragte. Der EDSA forderte die Aufsichtsbehörden in diesem Zusammenhang auf, über die Beantwortung der Fragen hinaus weitere Kommentare im Zusammenhang mit der Evaluierung der DS-GVO zu übersenden.

Bereits am 11. Juli 2018 hatte die DSK ihren Arbeitskreis für Grundsatzfragen beauftragt, einen Bericht aller deutschen Datenschutzaufsichtsbehörden zu verfassen, um auf eine entsprechende Anfrage der EU-Kommission vorbereitet zu sein. Der Landesbeauftragte entsandte einen Vertreter seiner Behörde in einen dazu gebildeten Unterarbeitskreis.

Die DSK verabschiedete anlässlich ihrer 98. Konferenz am 6. November 2019 den „Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO“[3], der – über die durch die EU-Kommission festgelegten Themen hinaus – insbesondere die Anwendungs- und Auslegungsprobleme mit der DS-GVO anhand von Erfahrungen aus der Beratung öffentlicher und nichtöffentlicher Verantwortlicher in den Blick nahm, um konkrete Änderungsbedarfe an der Verordnung zu formulieren. Dieser Erfahrungsbericht, der am 13. Dezember 2019 dem EDSA übersandt wurde, teilt die Auffassung des EDSA, dass sich die Regelungen der DS-GVO grundsätzlich bewährt haben und positive Effekte auf die Durchsetzung des Datenschutzes gezeigt haben; gleichzeitig sollten Verbesserungen im Detail vorgeschlagen werden.

Der Bericht gliedert sich in neun Schwerpunkte zu den Themen Alltagserleichterung und Praxistauglichkeit, Datenpannenmeldungen, Zweckbindung, Data Protection by Design, Befugnisse der Aufsichtsbehörden und Sanktionspraxis, Zuständigkeitsbestimmungen – Zusammenarbeit und Kohärenz, Direktwerbung, Profiling und Akkreditierung. Die Praxiserfahrungen der Aufsichtsbehörden decken sich weitestgehend mit den für den Bericht eingeholten Stellungnahmen der Wirtschaftsverbände. Nicht nur der Umfang der Pflichten der Verantwortlichen, sondern auch Unklarheiten und Auslegungsprobleme schlagen sich direkt in Beratungsbedarfen bzw. der Arbeitsbelastung der Aufsichtsbehörden nieder.

Der EDSA beschloss im Februar 2020 seinen Evaluierungsbericht; die nationale Stellungnahme der DSK ist diesem beigefügt. Dieser Bericht wurde der Europäischen Kommission übermittelt.

Die Bewertungen der Kommission werden wohl nicht zu schnellen Änderungsvorschlägen für den Text der DS-GVO führen. Vornehmlich geht es ihr um den Stand der Implementierung der DS-GVO und der JI-Richtlinie im nationalen Recht und die Durchsetzung der DS-GVO gegenüber global aufgestellten Internet-Konzernen im Rahmen der Zusammenarbeit der Aufsichtsbehörden.

In diesem letzteren Bereich sind insbesondere im Rahmen der Beschwerdebearbeitung erforderliche Maßnahmen bisher nicht zu verzeichnen gewesen. Dies hat einerseits bei der besonders sensibilisierten Öffentlichkeit als auch andererseits bei nationalen, zumal kleinen und mittleren Unternehmen den negativen Eindruck erweckt, dass gerade diese großen Internetkonzerne nicht wie erforderlich aufsichtsbehördlich kontrolliert werden und daher einen Wettbewerbsvorteil genießen. Dem EDSA wie auch der Europäischen Kommission ist diese Situation bekannt. Bei der Evaluierung dürfte daher auch die Frage nach einem strukturellen Defizit infolge der nicht gleichförmigen Anwendung des One-Stop-Shop-Prinzips zu behandeln sein.

[3] https://lsaurl.de/dsgvoerfahrungen

5 Weitere europäische und internationale Entwicklungen

5.1 Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA), der sich aus Vertretern der nationalen Behörden und des Europäischen Datenschutzbeauftragten (EDSB) zusammensetzt (vgl. zu dessen Aufgaben XV. Tätigkeitsbericht, Nr. 2.1), hat im Berichtszeitraum die Abarbeitung seines Arbeitsprogramms 2019/2020 zur einheitlichen Implementierung der europäischen Datenschutzregelwerke (DS-GVO und JI-Richtlinie) weit vorangetrieben.

Mit der Vorbereitung seiner Entscheidungen zu Leitlinien, Empfehlungen und bewährten Verfahren sowie – soweit erforderlich – der Beschlüsse in Kohärenzverfahren beauftragt der EDSA derzeit 13 Fachuntergruppen. Die Fachuntergruppen bestehen aus den von den Mitgliedern des Ausschusses bekannt gegebenen Bediensteten der Aufsichtsbehörden und des EDSB sowie aus Mitarbeitern des EDSA-Sekretariats, die die Fachuntergruppen unterstützen.

Im Rahmen von 56 im Arbeitsprogramm 2019/2020 festgeschriebenen einmaligen oder wiederkehrenden Aufgaben hat der EDSA in zehn Plenumssitzungen 66 Dokumente verabschiedet. Da der Ausschuss gegebenenfalls Konsultationen interessierter Kreise gem. Art. 70 Abs. 4 der DS-GVO durchführt, wurden einige der Dokumente zweimal beraten. Von den verabschiedeten Dokumenten sind vor allem die Folgenden zu erwähnen (die Arbeitssprache im EDSA ist Englisch):

- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects,
- Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities,
- Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR and related issues such as the preliminary vetting of complaints,
- Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679),
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,
- Guidelines 3/2019 on processing of personal data through video devices,
- Guidelines 3/2018 on the territorial scope of the GDPR (Article 3),
- Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1).

Die tägliche Rechtsanwendung und -praxis in den mitgliedstaatlichen Aufsichtsbehörden muss sich an diesen Vorgaben orientieren und ausrichten.

Die Vertretung der deutschen Aufsichtsbehörden im EDSA wird durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und einen Leiter einer Aufsichtsbehörde eines Landes (gemeinsamer Vertreter und Stellvertreter nach § 17 Abs. 1 BDSG) wahrgenommen. Dies ist derzeit der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. Bedauerlicherweise hat sich der Bundesrat noch nicht auf einen zu wählenden Vertreter der Länder einigen können.

Das Verfahren zur Herstellung eines gemeinsamen Standpunktes u. a. für die Stimmabgabe im EDSA ist in § 18 BDSG geregelt, dessen Gesetzesbegründung die Aufsichtsbehörden zur Sicherstellung eines konsistenten Standpunktes während des gesamten Verfahrens verpflichtet (diese Arbeit wird durch die Zentrale Anlaufstelle (ZASt) beim Bundesbeauftragten unterstützt, s. Nr. 5.2). Die Arbeit der deutschen Vertreter in den Fachuntergruppen des EDSA wird daher durch die 26 Arbeitskreise der DSK begleitet und unterstützt. Der Landesbeauftragte ist in den Arbeitskreisen vertreten und beteiligt sich entsprechend an der Beratung der europäischen Themen. Die Zuordnung der einzelnen Arbeitskreise zu den Fachuntergruppen des EDSA wird durch die Analyse der Arbeitsprogramme und die sich daraus ergebenden notwendigen Zuarbeiten weiterer Arbeitskreise ergänzt. Durch die Ausrichtung der Arbeitskreise auf die europäischen Diskussionen werden die Themen und Positionen der deutschen Aufsichtsbehörden in die Facharbeit auf europäischer Ebene frühzeitig eingebracht. Dadurch wird das Abstimmungsverhalten des Gemeinsamen Vertreters im EDSA nach Herstellung eines Gemeinsamen Standpunktes inhaltlich konsistent vorbereitet.

Der Landesbeauftragte nimmt an der Erarbeitung dieser Rechtsentwicklungen in den Arbeitskreisen der DSK teil, ist an den Entscheidungen des EDSA mittelbar beteiligt und berücksichtigt diese bei seiner Rechtsanwendung der DS-GVO.

5.2 Zusammenarbeit der Aufsichtsbehörden

Das Kapitel VII. der DS-GVO regelt „Zusammenarbeit und Kohärenz“. Demgemäß arbeiten die Aufsichtsbehörden auf europäischer Ebene vor allem in grenzüberschreitenden Fällen zusammen, indem sie sich informieren, durch Maßnahmen der Amtshilfe unterstützen, Entscheidungen im Konsens herbeiführen oder sogar gemeinsame Maßnahmen ergreifen.

Grenzüberschreitende Fälle sind solche, die einen Bedarf nach Abstimmung zwischen mindestens zwei europäischen Aufsichtsbehörden auslösen. Es handelt sich um Verstöße, die den Behörden entweder durch Beschwerden oder auf andere Art zur Kenntnis gelangen und die im Zusammenhang mit Tätigkeiten von Niederlassungen eines Verantwortlichen oder Auftragsverarbeiters in mehr als einem Mitgliedstaat stehen oder die Auswirkungen auf Betroffene in mehr als einem Mitgliedstaat haben oder haben können (Art. 4 Nr. 23 lit. a und b DS-GVO). Federführend zuständig ist dann immer die Aufsichtsbehörde am Ort der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters (One-Stop-Shop, Art. 56 Abs. 1 i. V. m. Art. 4 Nr. 16 lit. a und b DS-GVO).

Unterhalb der Schwelle dieser gesetzlich definierten grenzüberschreitenden Fälle gibt es eine Anzahl von Konstellationen, die zwei europäische Aufsichtsbehörden betreffen, jedoch keine einheitliche abgestimmte Entscheidung erfordern. Soweit z. B. lediglich eine einzelne Niederlassung in einem Mitgliedstaat die Rechte von Be-

troffenen in einem anderen Mitgliedstaat beeinträchtigt, liegt kein grenzüberschreitender, sondern vielmehr ein lokaler Fall vor, der an die Aufsichtsbehörde am Ort der Niederlassung abgegeben wird. Ebenfalls ein lokaler Fall ist in den Konstellationen gegeben, in denen die Zweigniederlassung vor Ort nur Betroffene vor Ort in ihren Rechten beeinträchtigt. Unter Berücksichtigung des Verfahrens nach Art. 56 Abs. 3 DS-GVO kann die Aufsichtsbehörde vor Ort den Fall selbst entscheiden.

Bevor eine Kommunikation auf europäischer Ebene über die Behandlung eines grenzüberschreitenden Falls beginnen kann, muss innerhalb der Bundesrepublik Deutschland die zuständige Aufsichtsbehörde ermittelt werden. Aus einem anderen Mitgliedstaat eingehende Beschwerden werden durch § 19 Abs. 1 BDSG in das Bundesland am Ort der Hauptniederlassung bzw. der einzigen Niederlassung verwiesen, soweit nicht der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig ist. Beschwerden, die von Deutschland in einen anderen Mitgliedstaat abgegeben werden, müssen vorher nach § 19 Abs. 2 BDSG in Anlehnung an das One-Stop-Shop-Prinzip ebenfalls dem Bundesland zugewiesen werden, in dem der Verantwortliche oder Auftragsverarbeiter eine Hauptniederlassung bzw. eine einzige Niederlassung (hilfsweise aber auch eine (Zweig)-Niederlassung) unterhält. Durch diese Regelungen wird eine unternehmensbezogene Konzentration der aufsichtsbehördlichen Bearbeitung innerhalb der Bundesrepublik erreicht, so dass die zuständige Behörde immer über die notwendigen Aufsichtsbefugnisse und Kenntnisse verfügt.

Die Kommunikation auf europäischer Ebene wird in der Internetanwendung „Internal Market Information System“ (IMI) organisiert (vgl. XV. Tätigkeitsbericht, Nr. 2.1). Zwischen dem 25. Mai 2018 und dem 31. Dezember 2019 wurden 807 grenzüberschreitende Kooperationsfälle registriert, deren einzelne Verfahrensschritte zu über 100.000 Systembenachrichtigungen per E-Mail an die Aufsichtsbehörden führten. Die federführenden Aufsichtsbehörden konnten 79 von 142 Verfahren nach Art. 60 DS-GVO in Form abschließender Entscheidungen zu Ende führen.

Nachdem der EDSA die in IMI abzuarbeitenden Verfahren in einer am 14. Mai 2019 verabschiedeten internen Leitlinie grundlegend beschrieben hatte („Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR and related issues such as the preliminary vetting of complaints“), regelte die DSK im November 2019, wie die deutschen Aufsichtsbehörden in den europäischen Verfahren zusammenarbeiten sollten. Die deutschen Aufsichtsbehörden werden zwar nach Art. 51 Abs. 3 DS-GVO i. V. m. § 17 Abs. 1 BDSG vom gemeinsamen Vertreter im Ausschuss vertreten und von der ZASt bei ihrer Arbeit unterstützt und koordiniert, sind jedoch im europäischen Verbund vollwertige, gleichberechtigte und unabhängige Aufsichtsbehörden. Jede Aufsichtsbehörde prüft daher anhand Art. 4 Nr. 22 DS-GVO die eigene Betroffenheit und meldet diese unter Angabe des einschlägigen Tatbestandes in IMI.

Für das weitere Verfahren (Art. 60 DS-GVO) haben sich die deutschen Aufsichtsbehörden mit dem Ziel eines einheitlichen Auftretens gegenüber den anderen Mitgliedstaaten darauf geeinigt, einer Aufsichtsbehörde mit einer Niederlassung (Hauptniederlassung, deutsche Hauptverwaltung, Niederlassung mit Schwerpunkt der Datenverarbeitung, Niederlassung mit dem größten Verarbeitungsumfang, hilfsweise das Bundesland mit den meisten Betroffenen oder einer besonderen Expertise) eine besondere Rolle zuzumessen. Diese Rolle besteht in der Information der anderen Auf-

sichtsbehörden, der Einbeziehung der eingehenden Stellungnahmen, der fachlichen Abstimmung mit den anderen Aufsichtsbehörden und in der Vornahme der Verfahrenshandlungen. Gelingt eine Verständigung über diese Fragen, verzichten die anderen betroffenen deutschen Aufsichtsbehörden auf inhaltliche Äußerungen gegenüber den anderen europäischen Behörden.

In vergleichbarer Weise haben sich die deutschen Aufsichtsbehörden – ebenfalls im November 2019 – auf ein abgestimmtes Vorgehen im Prozess zur Einleitung von Verfahren nach Art. 64 Abs. 2 DS-GVO geeinigt, welcher das Recht jeder Aufsichtsbehörde auf Anrufung des EDSA regelt. Auch hier bemühen sich die deutschen Aufsichtsbehörden im gesamtstaatlichen Interesse um ein einheitliches, verlässliches Auftreten und konsistentes Verhalten. So sollen sich die Aufsichtsbehörden vor Einleitung des Verfahrens nach Art. 64 Abs. 2 DS-GVO in Form eines Meinungsbildes abstimmen. Die initiierende Aufsichtsbehörde ist an die Einwände der anderen Aufsichtsbehörden nicht gebunden, aber gleichwohl gehalten, die eigene Entscheidung mitzuteilen und zu begründen.

Der Landesbeauftragte ist auf der einen Seite von grenzüberschreitenden Beschwerden betroffen, auf der anderen Seite wurden solche bei ihm eingereicht, so dass er an den oben beschriebenen Verfahren teilnimmt. Diese Tätigkeit ist aufgrund der vielen Fallgestaltungen komplex. Die europäische Zusammenarbeit und die darauf ausgerichtete innerdeutsche Koordinierung werden sich weiter verstärken.

5.3 Brexit

Das Vereinigte Königreich Großbritannien und Nordirland hat am 29. März 2017 den Austritt aus der Europäischen Union (EU) erklärt. Der dreimal verschobene Austrittstermin fiel nach Bewilligung durch den Europäischen Rat auf den 31. Januar 2020. Bereits am 14. November 2018 hatten sich die EU und die Regierung des Vereinigten Königreichs auf ein entsprechendes Austrittsabkommen geeinigt. In dem Abkommen ist eine Übergangsphase bis voraussichtlich 31. Dezember 2020 vorgesehen, in der das Vereinigte Königreich zunächst wie bisher alle EU-Regeln einhält und weiterhin Beiträge zahlen wird, aber in EU-Gremien keine Mitsprache mehr hat. Die anschließenden, langfristigen Beziehungen zwischen dem Vereinigten Königreich und der EU bleiben jedoch noch Gegenstand von Verhandlungen. Sollte bis Ende 2020 kein entsprechendes Abkommen in Kraft sein und die Übergangsphase nicht einvernehmlich verlängert werden, stünde ein ungeregelter Austritt ohne Abkommen bevor.

Im Falle eines ungeregelten Austritts (No-Deal-Brexit) würde das Vereinigte Königreich am 1. Januar 2021 ab 00:00 Uhr „Drittland“ im Sinne des Kapitels V der DS-GVO.

Mit Presseinformation vom 13. März 2019 und mit Informationen an die gewerblichen Kammern im Land Sachsen-Anhalt gab der Landesbeauftragte für den Datenschutz Hinweise für sachsen-anhaltische Unternehmen zur Vorbereitung auf einen ungeregelten Brexit. Unter Berücksichtigung der regionalen Wirtschaftsstruktur stellte der Landesbeauftragte speziell für die kleinen und mittleren Unternehmen mit Sitz oder Niederlassung in Sachsen-Anhalt vorsorglich die maßgeblichen Möglichkeiten dar, die Prozesse des grenzüberschreitenden Datenverkehrs auch nach einem ungeregelten Austritt datenschutzkonform weiterführen zu können.

Die DS-GVO hält ein Spektrum von Instrumenten zur Rechtfertigung von Datenübermittlungen in Länder außerhalb der EU vor. Neben altbewährten Instrumenten wie Angemessenheitsentscheidungen der EU-Kommission (Art. 45 DS-GVO), Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und lit. d DS-GVO) oder Binding Corporate Rules (Art. 46 Abs. 2 lit. b, Art. 47 DS-GVO) können Übermittlungen auch auf genehmigte Verhaltensregeln und Zertifizierungen (Art. 46 Abs. 2 lit. e und lit. f DS-GVO) gestützt werden.

Vorzugswürdig, weil mit relativ geringem Aufwand umsetzbar, dürfte regelmäßig die Vereinbarung von Standarddatenschutzklauseln sein.

Die Informationen enthielten darüber hinaus eine „Information note“ des Europäischen Datenschutzausschusses über Datentransfers im Rahmen der DS-GVO im Falle eines No-Deal-Brexits vom 12. Februar 2019 und den Beschluss der DSK vom 8. März 2019 „Informationen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden zu Datenübermittlungen aus Deutschland in das Vereinigte Königreich Großbritannien und Nordirland ab dem 30. März 2019“. Die Erläuterungen gelten für den nun späteren Austrittstermin fort.

5.4 Europarat – Datenschutzkonvention 108

Die ursprüngliche Europaratskonvention 108 zum Datenschutz wurde am 28. Januar 1981 zur Unterzeichnung aufgelegt. Sie war das erste rechtsverbindliche internationale Instrument im Bereich des Datenschutzes und bildete prinzipienbasiert das Verständnis darüber ab, wie ein Mindeststandard des Datenschutzes beim damaligen Stand der Digitalisierung von einem Staat zu regeln sei.

Der zwischenzeitlich eingetretene technische Fortschritt machte eine Überarbeitung der Konvention erforderlich, welche im Mai 2018 erfolgreich abgeschlossen wurde. Der Ratifizierungsprozess durch die 47 Mitgliedstaaten dauerte bis weit in das Jahr 2019. Durch die Änderung wurden Betroffenenrechte und Pflichten der verantwortlichen Stelle an die DS-GVO angepasst. Dazu gehören das Recht auf Information, ein Widerspruchsrecht sowie die Pflicht des Verantwortlichen, Verstöße an eine Aufsichtsbehörde zu melden, welche mit Kontroll- und Sanktionsbefugnissen auszustatten ist und mit anderen Aufsichtsbehörden grenzüberschreitend kooperieren muss. Da die Konventionen des Europarates völkerrechtlich verbindlich sind, sind die Unterzeichnerstaaten verpflichtet, soweit noch nicht geschehen, entsprechende Regelungen einzuführen.

5.5 Internationale Datenschutzkonferenz

Die 41. Internationale Datenschutzkonferenz in Tirana im Oktober 2019 mit Vertretern aus 80 Ländern stand unter dem Motto „Konvergenz und Konnektivität erhöhen die globalen Datenschutzstandards im digitalen Zeitalter“. Ziel war die stärkere globale Vernetzung des Datenschutzes, denn in Zeiten grenzüberschreitender Datenströme sind die Rechte der Datensubjekte nur durch grenzübergreifende Garantien zu schützen. Die Konferenz verabschiedete verschiedene Entschließungen, u. a. eine „Internationale Entschließung über das Recht auf Privatsphäre als grundlegendes Menschenrecht und als Voraussetzung für die Wahrung anderer Grundrechte“. Mit dieser Entschließung werden die Regierungen weltweit aufgefordert, Datenschutz als grundlegendes Menschenrecht anzuerkennen und im nationalen Recht aufzuneh-

men. Darüber hinaus sollen die Unternehmen mehr Verantwortlichkeit für den Datenschutz und den Schutz weiterer Grundrechte übernehmen. Für den Bereich der Europäischen Union ist dies mit der DS-GVO bereits weitgehend auf den Weg gebracht.

Die Konferenz strebt eine festere Struktur mit jährlichen Treffen an und hat Arbeitsschwerpunkte für den Zeitraum bis zum Ende des Jahres 2021 beschlossen, darunter das Thema Künstliche Intelligenz.

6 Technik und Organisation

6.1 E-Government-Gesetz Sachsen-Anhalt – Sachstand

Der Landesbeauftragte hat sich in den zurückliegenden Tätigkeitsberichten (XIII./XIV. Tätigkeitsbericht, Nr. 4.4; XV. Tätigkeitsbericht, Nr. 5.3) umfänglich mit dem langwierigen Gesetzgebungsprozess und kritisch mit den Inhalten des damaligen Gesetzentwurfs der Landesregierung (LT-Drs. 7/1877) auseinandergesetzt.

Nach der nochmaligen Überarbeitung des Gesetzentwurfs durch die Koalitionsfraktionen und Beratungen in den Ausschüssen für Inneres und Sport, für Wirtschaft, Wissenschaft und Digitalisierung sowie für Finanzen wurde am 19. Juni 2019 das Gesetz zur Förderung der elektronischen Verwaltung des Landes Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt – EGovG LSA) durch den Landtag beschlossen.

Damit verfügt nun auch das Land Sachsen-Anhalt, wenn auch als eines der letzten Länder, über ein modernes und bürgerfreundliches E-Government-Gesetz, welches am 31. Juli 2019 in Kraft getreten ist (GVBl. LSA S. 200).

Das EGovG LSA ist ein wesentlicher Bestandteil der Digitalen Agenda des Landes. Als Organisations- und Verwaltungsgesetz regelt es sowohl das rechtssichere elektronische Verwaltungshandeln als auch die künftige Organisation und Koordinierung der Informations- und Kommunikationstechnologie für die gesamte Landesverwaltung, insbesondere auch für die Kommunen. Diese werden mit dem Gesetz insgesamt verbindlicher in das System des E-Government eingebunden.

Wichtige Regelungen betreffen u. a.:

- Einführung der elektronischen Aktenführung und Vorgangsbearbeitung (§ 3),
- Verschlüsselung bei der elektronischen Kommunikation (§ 8),
- Elektronische Kommunikation zwischen den Behörden untereinander und mit natürlichen oder juristischen Personen des Privatrechts (§§ 9 - 12),
- Landesportal Sachsen-Anhalt als zentrales Verwaltungsportal der Landesverwaltung zur Umsetzung des Onlinezugangsgesetzes (§ 16) – s. Nr. 6.2 –,

- Bereitstellung von Basisdiensten (u. a. Nutzerkonten, sichere Übertragungswege, elektronische Bezahlmöglichkeiten, elektronische Beteiligungsverfahren) (§ 17),

- Einrichtung eines Beauftragten der Landesregierung Sachsen-Anhalt für Informations- und Kommunikationstechnologie (§ 13),

- Schaffung eines IT-Kooperationsrats Sachsen-Anhalt zur verwaltungsträgerübergreifenden Zusammenarbeit insbesondere zwischen Land und Kommunen (§ 24).

Der Landesbeauftragte ist beratendes Mitglied dieses IT-Kooperationsrats (§ 24 Abs. 2 Satz 2 EGovG LSA). Der IT-Kooperationsrat soll Empfehlungen zu im IT-Planungsrat zu behandelnden Themen und zur strategischen Entwicklung der Informationstechnologie geben. Einen ersten Schwerpunkt wird die Kommentierung der seit langem ausstehenden E-Government-Strategie bilden. Die konstituierende Sitzung des IT-Kooperationsrats fand am 13. November 2019 im Ministerium der Finanzen, unter Leitung des Ministers der Finanzen als Landesbeauftragten für IKT, statt.

6.2 Onlinezugangsgesetz und Portalverbund

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsdienstleistungen (Onlinezugangsgesetz – OZG) vom 14. August 2017 (BGBl. I S. 3122, 3138) trat am 18. August 2017 in Kraft. Der Landesbeauftragte hatte schon damals im Rahmen des Gesetzgebungsverfahrens zum E-Government-Gesetz Sachsen-Anhalt auf die Anforderungen aus dem OZG für ein zukunftsfähiges E-Government hingewiesen.

Das OZG trifft wesentliche Regelungen zu (vgl. XV. Tätigkeitsbericht, Nr. 5.4):

- **Online-Services** – bis 31. Dezember 2022 sollen alle Verwaltungsleistungen auch online bereitstehen,

- **Portalverbund** – Bund und Länder sollen ihre Portale zu einem übergreifenden Portalverbund verknüpfen,

- **Nutzerkonten** – Nutzerinnen und Nutzer müssen sich für alle Leistungen im Portalverbund mit einem Nutzerkonto einheitlich identifizieren können,

- **Standards** – der Bund erhält die Möglichkeit, Vorgaben für IT-Anwendungen, Basisdienste sowie Standards für Schnittstellen und Sicherheitsvorgaben zu machen.

Mit Stand April 2018 umfasste der OZG-Umsetzungskatalog insgesamt 575 Verwaltungsleistungen für Bürgerinnen und Bürger sowie Unternehmen. Diese sind anhand von Lebens- und Geschäftslagen identifiziert und systematisiert worden. Ausgangspunkt für die Identifikation der umzusetzenden Verwaltungsleistungen bildete der Leistungskatalog der öffentlichen Verwaltung. Diese identifizierten Leistungen wurden zu 14 Themenfeldern zusammengefasst. Für jedes Themenfeld übernehmen ein Land und das zuständige Bundesressort die Federführung.

In sog. „Digitalisierungslaboren“ arbeiten Bund, Länder und Kommunen zusammen. Ziel ist es, Online-Angebote zu konzipieren und ggf. zu entwickeln, die danach von anderen Ländern nachgenutzt werden können. Bundesregierung und Landesregierungen haben sich bei der Umsetzung des OZG auf die Anwendung des „Einer-für-Alle-Prinzips“ verständigt, d. h. ein Hauptverantwortlicher prüft das Verfahren und alle anderen übernehmen es anschließend.

Das Land Sachsen-Anhalt hat die Federführung für das Themenfeld „Bildung“ übernommen. Darin sind insgesamt 29 Verwaltungsleistungen enthalten. Das erste zu prüfende OZG-Projekt betrifft das Online-Verfahren zum BAföG.

Der Landesbeauftragte wirkt bei der Umsetzung der OZG-Projekte in Sachsen-Anhalt im Rahmen seiner personellen Kapazitäten auf die Einhaltung datenschutzrechtlicher Vorgaben hin.

6.3 Verwaltungs- und Registermodernisierung – datenschutzkonform gestalten

Mit der Verabschiedung des OZG ist eine fundamentale Veränderung der Verwaltung in Bund, Ländern und Kommunen in Deutschland verbunden. Auf der Grundlage des OZG sollen bis zum Ende des Jahres 2022 die wesentlichen Verwaltungsleistungen vollständig digitalisiert werden – deutschlandweit. Ziele dieses umfassenden Transformationsprozesses der deutschen Verwaltung sollen leistungsfähige Online-Services, d. h. online verfügbare Verwaltungsleistungen für Bürgerinnen und Bürger sowie Unternehmen, ein Verwaltungsebenen übergreifender Portalverbund und der Gebrauch und die Identifizierung über ein einheitliches Nutzer- bzw. Unternehmenskonto, sein (vgl. Nr. 6.2).

Das vom Normenkontrollrat (NKR) im Oktober 2017 veröffentlichte Gutachten „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.“ widmet sich der Modernisierung der stark zersplitterten Registerlandschaft in Deutschland, die bei der umfassenden Digitalisierung der Bundes- und Landesverwaltungen ein wirksames E-Government für Bürgerinnen und Bürger sowie Unternehmen bisher stark behindert. Das Gutachten wurde im Auftrag des NKR von der Unternehmensberatung McKinsey & Company in Zusammenarbeit mit dem Statistischen Bundesamt und der Deutschen Universität für Verwaltungswissenschaften Speyer erstellt.

Der NKR kommt in seinem Gutachten zu dem Ergebnis, dass in Deutschland erheblicher Modernisierungsbedarf bestehe. Register sollen über standardisierte digitale Schnittstellen zugänglich gemacht werden und die Verknüpfbarkeit sowie Qualität der Daten zentral gesteuert werden können. Moderne Register bilden die unverzichtbare Basis für ein wirksames E-Government. Eine Analyse auf Basis der Erfüllungsaufwandsmessungen des Statistischen Bundesamts zeige, dass bei einer vollständigen Digitalisierung der Top-35-Verwaltungsleistungen für Bürger eine Zeitersparnis von 47% für Behördengänge zu erwarten sei.

Die zehn „Kernbotschaften“ des NKR-Gutachtens lauten:

1. Moderne Register sind das Fundament besserer Verwaltungsleistungen für Bürger und Unternehmen. Ohne moderne Register sind effiziente, bürger- und unternehmensfreundliche digitale Angebote nicht möglich.

2. Die deutsche Registerlandschaft erfüllt die nötigen Anforderungen derzeit nicht. Es besteht umfassender Modernisierungsbedarf. Die Registerlandschaft in Deutschland ist administrativ zersplittert. Es gibt mehr als 200 Register, viele davon noch einmal nach örtlicher Zuständigkeit untergliedert und unterschiedlich ausgestaltet.

3. Moderne Register ermöglichen erhebliche Einsparungen. Die Digitalisierung der wichtigsten Verwaltungsleistungen auf Basis moderner Register entfaltet bei einmaligen Investitionskosten in Höhe von ca. 2,5 Mrd. EUR ein Entlastungspotenzial von ca. 6 Mrd. EUR pro Jahr.

4. Moderne Register schaffen eine tragfähige Grundlage für staatliche Entscheidungen und offene Verwaltungsdaten (Open Data). Register enthalten wichtige amtliche Informationen und sind Grundlage der öffentlichen Statistik sowie staatlicher Planungs-, Entscheidungs- und Steuerungsprozesse.

5. Andere Länder machen erfolgreich vor, wie es geht. Deutschland darf den Anschluss an die Digitalisierungspioniere nicht verpassen und sollte sich bei der Modernisierung seines Registerwesens an erfolgreich etablierten Lösungen orientieren. Beispiele sind die datenschutzkonforme Verknüpfung von Personendaten in Estland und Österreich, die dezentrale, aber harmonisierte Registerführung in der Schweiz, das sogenannte „Once Only“-Prinzip für Basisdaten in Dänemark sowie die vollständige Digitalisierung komplexer Verwaltungsleistungen durch vernetzte Register in Schweden.

6. Kern moderner Register sind gute Basisdaten, die von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only“). Häufig gebrauchte Basisdaten zu Personen, Firmen, Kraftfahrzeugen sowie Orten und Immobilien sollten von Bürgern und Unternehmen in Zukunft nur einmal angegeben werden müssen.

7. Wirklich medienbruchfrei werden digitale Verwaltungsverfahren erst dann, wenn neben den Basisdaten noch weitere Registerinformationen ausgetauscht werden können. Für viele Verwaltungsleistungen sind neben den Basisdaten weitere Informationen erforderlich.

8. Die datenschutzkonforme Verknüpfung von Registerdaten ist möglich. Bürger und Unternehmen erhalten mehr Transparenz und Kontrolle über ihre Daten. Viele der positiven Effekte einer modernisierten Registerlandschaft stellen sich erst ein, wenn Registerdaten verknüpfbar sind. Ein verschlüsseltes Personenkennzahlensystem in Anlehnung an das Modell Österreichs macht dies möglich und trägt den Urteilen des Bundesverfassungsgerichts zum Datenschutz angemessen Rechnung. Gleichzeitig schafft es für Bürger eine größere Transparenz über den Zugriff auf ihre Daten und verbessert so den Schutz personenbezogener Informationen.

9. Es braucht eine zentrale Stelle, um die Registermodernisierung zu steuern, und eine politische Verantwortlichkeit auf höchster Ebene. Die notwendige Standardisierung, Harmonisierung und Konsolidierung der deutschen Registerlandschaft erfordert eine übergreifende Steuerung. Nötig ist eine zentrale Koordinierungsstelle mit starken Kompetenzen und ausreichenden Ressourcen.

10. Zügiges und mutiges politisches Handeln ist gefragt: Es braucht ein Registermodernisierungsgesetz. Die Bundesregierung sollte zügig ein Registermodernisierungsgesetz vorlegen, das den nötigen politischen Willen unterstreicht und die Grundlage für die weitere Umsetzung schafft. Die Registermodernisierung muss eigenständiger Bestandteil der nächsten Digitalisierungsagenda werden und eng mit der Umsetzung des Onlinezugangsgesetzes, der Einführung eines Portalverbundes und der Konzeption von Servicekonten verbunden werden.

Das Bundesministerium des Innern, für Bau und Heimat (BMI) legte im März 2019 prioritäre digitale Themen zur Modernisierung der Verwaltung vor:

- Sicherheit im Netz auf höchstem Niveau,
- moderne Verwaltung, die Bürgern und der Wirtschaft dient,
- starke Zivilgesellschaft, welche sich die Digitalisierung zunutze macht sowie
- ethische Leitlinien für die Digitalisierung und eine moderne Datenpolitik.

Der IT-Planungsrat hat sich auf seiner 28. Sitzung im März 2019 mit dem Thema Registermodernisierung befasst. Er beschloss hierzu ein Koordinierungsprojekt „Registermodernisierung“ unter Federführung des Bundes, Hamburgs und Bayerns sowie unter Einbeziehung der Koordinierungsstelle für IT-Standards (KoSIT), des Aufbaustabs Föderale IT-Kooperation (FITKO) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Auf seiner 29. Sitzung im Juni 2019 beauftragte der IT-Planungsrat das Koordinierungsprojekt „Registermodernisierung“ insbesondere mit folgenden Aufgaben:

- Identifizierung der Anforderungen an eine Registermodernisierung,
- Erstellung eines Architekturmodells für eine Registerlandschaft auf der Basis vernetzter Register,
- Erfassung der Anforderungen für gesetzliche Änderungen,
- Erstellung eines Zielbildes und einer konkreten Maßnahmenplanung.

Die Diskussion um die Einführung eines die Register erschließenden, einheitlichen Personenkennzeichens ist in Deutschland nicht neu. Bereits in den 1970er Jahren stand das Thema auf der Agenda des Bundesministeriums des Innern und des Parlaments. Schon zur damaligen Zeit gab es aber verfassungsrechtliche Bedenken. Spätestens mit dem sog. Volkszählungsurteil des Bundesverfassungsgerichts von

1983 wurde einem verwaltungsübergreifenden Personenkennzeichen eine Absage erteilt.

Aus diesen gegebenen Anlässen hat die DSK am 12. September 2019 mit einer Entschließung nachdrücklich eine datenschutzkonforme und bürgerfreundliche Gestaltung bei der Digitalisierung der Verwaltung und konkret die Anwendung sektorspezifischer Identifikationskennzeichen eingefordert (**Anlage 5**).

Das an sich sinnvolle „Once Only"-Prinzip für die Inanspruchnahme von Verwaltungsleistungen könnte durch ein einheitliches, verwaltungsübergreifendes Personenkennzeichen konterkariert werden, weil hierdurch Gefährdungen des Persönlichkeitsrechts bzw. der informationellen Selbstbestimmung drohen. In den Beratungen auf Bundesebene wird die Verwendung der steuerlichen Identifikationsnummer favorisiert. Ob ein sog. „Datencockpit" hinreichende Garantien für den Grundrechtsschutz, insbesondere gegen beliebigen staatlichen Zugriff und Abgleich bieten kann, ist fraglich.

6.4 Standard-Datenschutzmodell 2.0a

Die Anwendungsbereiche des Standard-Datenschutzmodells (SDM) sind Planung, Einführung und Betrieb von Verarbeitungstätigkeiten, mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verarbeitungen) sowie deren Prüfung und Beurteilung. Damit unterstützt das SDM Verantwortliche in Wirtschaft und Verwaltung, die von der DS-GVO auferlegten Nachweis- und Rechenschaftspflichten zu erfüllen.

Die 98. DSK hat im November 2019 mit der Version 2.0a[4] eine grundlegend überarbeitete Version des SDM verabschiedet (vgl. zur Version 1.1 XIII./XIV. Tätigkeitsbericht, Nr. 4.1).

Die rechtlichen Anforderungen der DS-GVO werden vom SDM nun vollständig erfasst und mit Hilfe von sieben Gewährleistungszielen systematisiert. Der Katalog generischer Maßnahmen ermöglicht einen Einstieg in die praktische Anwendung des SDM. Das im SDM beschriebene Datenschutzmanagement führt Verantwortliche durch alle Phasen der Verarbeitung personenbezogener Daten und ermöglicht somit auch die kontinuierliche Aufrechterhaltung einer rechtssicheren Verarbeitung.

Mit dem SDM stellt die Konferenz eine Methode bereit, mit der die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird. Diese Maßnahmen sollen sicherstellen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DS-GVO erfolgt. Das SDM bietet mit seinen Gewährleistungszielen eine Transformationshilfe zwischen Recht und Technik und unterstützt damit einen ständigen Dialog zwischen Beteiligten aus den juristischen und technisch-organisatorischen Bereichen.

Das SDM hat nunmehr auch Eingang in das IT-Grundschutzkompendium 2019 des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) gefunden. Am 27. September 2019 veröffentlichte das BSI den IT-Grundschutzbaustein

[4] https://lsaurl.de/sdm20

CON.2 Datenschutz. Ziel des Bausteins ist es, die Verbindung der Anforderungen des SDM zum IT-Grundschutz darzustellen. Von zentraler Bedeutung ist dabei der Artikel 5 DS-GVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise als Schutzziele ausgewiesen sind.

Der Baustein CON.2 Datenschutz dient dem Verantwortlichen oder dem Auftragsverarbeiter zur Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen eine Verarbeitung und sonstige Nutzung personenbezogener Daten erfolgt. Hierbei sollte auch geprüft werden, ob dieser Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Behörde, Institution oder Unternehmen anzuwenden ist.

Die DSK empfiehlt den Verantwortlichen in Wirtschaft und Verwaltung, das SDM bei Planung, Einführung und Betrieb von personenbezogenen Verarbeitungen anzuwenden. Das SDM soll kontinuierlich weiterentwickelt werden. Anwenderinnen und Anwender sind eingeladen, den Datenschutzaufsichtsbehörden ihre Erfahrungen bei der Nutzung des SDM mitzuteilen, um zu einer stetigen Verbesserung des Modells beizutragen.

6.5 Biometrische Analyse

Erfassung und Auswertung biometrischer Merkmale sind vielfach ohne Wissen und Einverständnis der Betroffenen möglich. Videoüberwachungsanlagen können „unbemerkbar“ z. B. Alter, Geschlecht oder Gesichtsausdrücke und Blickrichtungen ermitteln, Profile bilden und Kunden wiedererkennen. Derzeit dient dies nur der passgenauen und gezielten Ansprache. Zukünftig ist es aber auch denkbar, dass Kunden gezielt bis hin zum Kauf eines gar nicht gewollten Produkts beeinflusst werden. Unerwünschte Kunden werden dezent zum Ausgang oder Nachbargeschäft geleitet, andere gezielt zum vorausgewählten Produkt. Neben solchen Anwendungen zu Werbezwecken dienen biometrische Systeme oftmals Identitätsfeststellungen und Zugangskontrollen.

Die DSK beschloss Anfang April 2019 ein Positionspapier zur biometrischen Analyse[5]. In diesem werden systematisch biometrische Merkmale betrachtet, die Leistungsfähigkeit zugehöriger Sensoren und Geräte analysiert, Verarbeitungsziele anhand von Einsatzszenarien erfasst und rechtlich bewertet und daraus Empfehlungen zur Gestaltung von konkreten Verfahren abgeleitet. Unerlaubte Szenarien sollen mit dem passenden Werkzeug „Datenschutz“ in ihre Grenzen verwiesen werden.

Im Mittelpunkt der rechtlichen Bewertung steht immer die Unterscheidung, ob die Auswertung der biometrischen Merkmale der eindeutigen Identifizierung der betroffenen Person im Sinne des Art. 9 Abs. 1 DS-GVO dient oder nicht. In ersterem Fall, etwa bei einer Zutrittsberechtigung, kommt Art. 9 Abs. 2 DS-GVO zur Anwendung. Neben wenigen benannten Ausnahmen bleibt im Wesentlichen nur die informierte, ausdrückliche Einwilligung der Betroffenen in die biometrische Analyse als Rechtsgrundlage. Im zweiten Fall ist Art. 6 Abs. 1 Satz 1 DS-GVO die Rechtsgrundlage und es kann sich gem. lit. f die Zulässigkeit aus einer Interessenabwägung, ggf. unter Einbeziehung von technischen und organisatorischen Maßnahmen, ergeben.

[5] https://lsaurl.de/popabio

6.6 Akkreditierung und Zertifizierung

Die DS-GVO sieht die Möglichkeit des Inverkehrbringens von Datenschutz-Siegeln (Art. 42 DS-GVO) durch fachkundige Zertifizierungsstellen (Art. 43 DS-GVO) vor. Ziel ist es, durch ein Gütesiegel zu beglaubigen, dass die geprüften Produkte und Verfahren den gesetzlichen Datenschutzanforderungen gerecht werden. Bei der Feststellung, ob die Zertifizierungsstellen selbst die nötige Fachkunde besitzen, werden zukünftig europaweit die jeweils zuständigen Datenschutzaufsichtsbehörden einbezogen. Diese sorgen mit dafür, dass die datenschutzrelevanten Kriterien passend aufgestellt und dauerhaft eingehalten werden.

Dazu ist in Deutschland eine Zusammenarbeit mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) vorgesehen. Diese führt in ihrer Funktion als nationale Akkreditierungsstelle der Bundesrepublik Deutschland die Akkreditierung von Zertifizierungsstellen im Bereich des Datenschutzes nach der Vorgabe der Verordnung (EG) Nr. 765/2008 und nach Maßgabe des deutschen Akkreditierungsstellengesetzes durch. Damit bestätigt sie, dass diese Stellen ihre Aufgaben fachkundig und nach geltenden Anforderungen erfüllen. Die DAkkS prüft also die Prüfer. Die Datenschutzaufsichtsbehörde prüft die Aussagen zum Datenschutz in den Kriterienkatalogen und Zertifizierungsprogrammen.

Wenn eine Firma Datenschutz-Gütesiegel erteilen, d. h. selbst eine Zertifizierungsstelle werden will, dann muss sie ihre im Zertifizierungsprogramm genannten Kriterien und Prüfverfahren mit der DAkkS und der zuständigen Datenschutzaufsichtsbehörde abstimmen. Die DAkkS akkreditiert nach DIN EN ISO/IEC 17065, die Datenschutzaufsichtsbehörde zertifiziert auf Basis dieser Akkreditierung gem. Art. 42 Abs. 5 DS-GVO.

Im Arbeitskreis Akkreditierung der DSK erfolgten allgemeine Koordinierungen zu den generellen Voraussetzungen und Kriterien. Im Berichtszeitraum wurden Schulungen durch die DAkkS durchgeführt, da Fachbegutachter benötigt werden, welche die Zertifizierungsstellen und ihre Zertifizierungsprogramme prüfen können. Ein Kooperationsvertrag, der Details der Zusammenarbeit von DAkkS und Datenschutzaufsichtsbehörden (Bereitstellung von Fachpersonal durch die Aufsichtsbehörden, Abläufe, Austausch von Mitarbeitern, Gebühren) regelt, wurde im Januar 2020 unterzeichnet.

Eine zukünftige Herausforderung werden Datenschutz-Siegel solcher Stellen sein, die zwar mit Datenschutz werben und mit entsprechenden Gütesiegeln Geld verdienen, oft sogar mit den gesetzlichen Regelungen für das jeweilige Siegel werben, aber nicht offiziell akkreditierte oder zertifizierte Stellen sind und sich meist auch nicht an die DS-GVO halten und so z. B. auf die Unterrichtung der zuständigen Aufsichtsbehörde nach Art. 43 Abs. 1 DS-GVO verzichten. Derzeit gibt es noch keine genehmigten nationalen Kriterien-Kataloge bzw. fertigen Vorgaben für Prüfungen von Kriterienkatalogen. In Sachsen-Anhalt hat noch keine Zertifizierungsstelle eigene Prüfkriterien zwecks Akkreditierung eingereicht.

6.7 Update und Ablösung veralteter Betriebssysteme und Standardsoftware

Die Pflicht zum regelmäßigen Schließen von Sicherheitslücken in Betriebssystemen und Standardsoftware durch das zeitnahe Einspielen von Updates und Patches des Herstellers ergibt sich aus Art. 5 Abs. 1 lit. f DS-GVO. Personenbezogene Daten

müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Dazu gehört auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. So können die Grundsätze Vertraulichkeit und Integrität gewahrt werden.

Werden bekannte Sicherheitslücken nicht geschlossen, sind die betroffenen Systeme potentiellen Angriffsvektoren ausgesetzt, auch wenn Firewall und Antivirensoftware installiert und nur eingeschränkte Benutzerkonten aktiv sind. Sicherheitslücken in Betriebssystemen und Standardsoftware können es Angreifern ermöglichen, Administrationsrechte zu erlangen, Sicherheitsmechanismen zu deaktivieren und unbemerkt weiteren Schadcode einzuschleusen oder Daten abwandern zu lassen. Dadurch können die Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung personenbezogener Daten, deren Gewährleistung durch Art. 32 Abs. 1 lit. b DS-GVO gefordert wird, erheblich gefährdet werden.

Jedes veröffentlichte Update gibt Aufschluss darüber, welche Sicherheitslücken damit geschlossen wurden. Aktuelle Betriebssysteme und Standardsoftware sind oft im Kern und in vielen Funktionalitäten identisch zu ihren Vorgängern. Veröffentlichte Updates für diese Produkte verraten immer auch neue Sicherheitslücken in den veralteten Vorgängerprodukten, für die keine Updates mehr zur Verfügung gestellt werden. Daher ist es sehr riskant, veraltete Betriebssysteme und Softwareprodukte einzusetzen, für die der Hersteller keine Sicherheitsupdates mehr liefert. In diesen Fällen ist eine Ablösung veralteter Betriebssysteme und Softwareprodukte dringend geboten.

Derzeit betrifft dies insbesondere die Betriebssysteme Windows 7, Windows Server 2008 und Windows Server 2008 R2 sowie die Softwareprodukte Microsoft Office 2010, SharePoint Server 2010 sowie SQL Server 2008 und 2008 R2. Alle diese Produkte erhalten ab Januar 2020 keine Sicherheitsupdates vom Hersteller Microsoft mehr (Office und SharePoint erst ab Oktober 2020) und sind daher zeitnah durch Alternativen oder Nachfolgeprodukte zu ersetzen (vgl. zu Windows 10 Nr. 6.8).

Für Windows 7 hat der Hersteller Microsoft aufgrund der starken Verbreitung des Betriebssystems eine Sonderlösung angeboten. Unternehmen, Vereine, Behörden und Bildungseinrichtungen können mit dem Hersteller gegen ein Entgelt eine gesonderte Supportverlängerung um bis zu 3 Jahre vereinbaren. In diesem Fall wird der Hersteller weiterhin Sicherheitsupdates jedoch nur direkt für die Abonnenten der Supportverlängerung bereitstellen. Aus Sicht des Landesbeauftragten ist dies jedoch keine nachhaltige Lösung.

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 BSI[6], Datenschutz-Folgenabschätzung im Auftrag der niederländischen Regierung 2018, Prüfbericht[7] des Bayerischen Landesamts für Datenschutzaufsicht 2017, Aktualisierung in dessen 9. Tätigkeitsbericht 2019[8], 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 weiternutzen. 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.

Telemetriedaten sind Daten, die aus dem laufenden System zum Hersteller in die USA übertragen werden, um diesem die Fehlersuche und die Optimierung und Verbesserung des Produkts „Windows“ (und auch der Anwendungen des Herstellers) zu erleichtern. Oft wird gefragt, ob das überhaupt personenbezogene Daten seien. Fakt ist: Telemetriedaten lassen sich nur personenbezogen sinnvoll auswerten. Der Anbieter einer Software will keine Statistik, um einen Fehlerort (z. B. beim Abstürzen eines Programms) einzugrenzen, sondern den Fehler direkt beheben und braucht dazu weitere Kontextinformationen wie installierte Produkte und Treiber, gleichzeitig laufende Programme, Prozesse und Anwendungen, bis hin zu den Inhalten von Datenfeldern oder der Zwischenablage. Da Microsoft die wichtigen Quelltexte nicht an die Nutzer herausgibt, kann auch nur Microsoft selbst mit diesen Kontextinformationen einen Fehler beheben. Je mehr Daten übermittelt werden, desto einfacher ist es für Microsoft. Telemetriedaten sind auch deshalb personenbezogen, da oft Profile gebildet werden müssen, denn ein erfahrener Nutzer bedient das System anders als

[6] https://lsaurl.de/sisyphus

[7] https://lsaurl.de/win10report

[8] https://lsaurl.de/ldatb2019

ein Neuling. Oft führen auch Ketten von Aktionen zu unerwarteten Ereignissen; auch solche Aktionen müssen im Profil chronologisch nachvollziehbar sein.

Es werden also Daten aller Art, insbesondere auch personenbezogene Daten (Art. 4 Nr. 1 DS-GVO) übertragen. Die explizit untersagte Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) kann dabei nicht ausgeschlossen werden, da auch Inhaltsdaten Fehler erzeugen könnten. Was ist nun zu tun? Microsoft könnte die Telemetriedaten-Übertragung abschaltbar gestalten. Das empfiehlt auch der Landesbeauftragte. Andernfalls ist eine transparente Gestaltung der Übertragungen insbesondere hinsichtlich der übertragenen Inhalte notwendig. So könnten „Fehler- und Absturzberichte“ explizit durch den Nutzer kontrolliert und das Absenden von Telemetriedaten bestätigt werden. Grundlage für die Datenübertragung ist eine informierte, freiwillige Einwilligung (Art. 4 Nr. 11, Art. 7 DS-GVO). Diese ist aber als Rechtsgrundlage für Behörden oder Schulen generell nicht geeignet.

Der Landesbeauftragte beteiligt sich an der Erarbeitung eines gemeinsamen Standpunktes der DSK und wird danach weitere Empfehlungen geben. Zur Erleichterung der Bewertung der Einhaltung der datenschutzrechtlichen Vorgaben der DS-GVO bei Windows 10 hat die DSK einstweilen ein Prüfschema „Datenschutz bei Windows 10“[9] veröffentlicht. In diesem wird ein Überblick über Windows und die datenschutzrelevanten Besonderheiten gegeben und aufgezeigt, welche Normen der DS-GVO auf Einhaltung zu überprüfen sind. Dann werden die genannten Prüfpunkte in einem Flussdiagramm als Übersicht vorgestellt. Mit Hilfe des Schemas ist es dann möglich, die Rechtsgrundlagen systematisch zu prüfen und die Frage, ob Windows 10 im geprüften Kontext eingesetzt werden darf, zu beantworten.

Untersuchungen Ende 2019 unter anderem durch das Bayerische Landesamt für Datenaufsicht 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 datenschutzkonforme 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.

---

[9] https://lsaurl.de/win10dspruef

Möglich ist auch die Konfiguration in vom Internet getrennten Netzwerken oder der Betrieb von Windows 10 in isolierten, virtuellen Maschinen. Dabei muss beachtet werden, dass wichtige Funktionen wie z. B. die Aktualisierung von Wurzelzertifikaten oder Prüfungen der Zertifikate ohne Internet nicht nutzbar sind. Solche Funktionen sind dann anderweitig bereitzustellen (Tunnel, Remote-Controlled Browser System, Drittanbietersoftware).

Eine schwächere Lösung besteht darin, Fachanwendungen, Datenbanken und Dokumente vom Betriebssystem logisch getrennt abzulegen; nur bei Aktualisierungen der Software bzw. Zugriffen auf das Internet sind diese Anwendungen und ihre Daten z. B. über genutzte Freigaben vorab zu deaktivieren.

Office 365

Die Nutzung der allgemeinen Microsoft Cloud in Form von Office 365 (nicht mehr innerhalb der „Microsoft Cloud Deutschland“, vgl. XIII./XIV. Tätigkeitsbericht, Nr. 9.2.5) konnte bisher ebenfalls noch nicht abschließend bewertet werden. Problematisch ist insbesondere die Nutzung der Microsoft Cloud-Dienste, die im Abonnement Office 365 integriert sind, wie OneDrive, Skype, Teams, Outlook oder die browserbasierten Versionen von Word, Excel usw. Für die Verantwortlichen ist nicht transparent, ob die Anwendungen noch in eigener Verantwortung (On Premises) betrieben werden oder ein Übergang zum Dienstleister Microsoft stattfindet, da lokale Datenverarbeitung medienbruchfrei und oberflächenintegriert in cloudbasierte Verarbeitungsformen überführt wird.

Die DSK arbeitet an einer datenschutzrechtlichen Bewertung der Vertragsinhalte (Online Service Terms) von Microsoft Office 365 hinsichtlich ihrer Konformität zu einem Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO.

Generell besteht bei Office 365 das Problem, dass der Verantwortliche die Datenverarbeitungen bei Microsoft nur unzureichend steuern kann. Insofern kann er seinen Verpflichtungen aus Art. 28 DS-GVO nicht hinreichend nachkommen. Öffentliche Einrichtungen haben eine besondere Verantwortung, die rechtliche Zulässigkeit der Verarbeitung personenbezogener Daten sicherzustellen.

Davon unabhängig könnte der Nutzer die Kontrolle über seine Daten aktuell nur behalten, wenn zur Installation der Software eine entsprechende On Premises-Lösung – also lokal installierte Software ohne Nutzung der Cloud Services und ohne Anbindung an ein Online-Konto – genutzt wird. Dabei betreibt der Lizenznehmer die Software in eigener Verantwortung auf seiner eigenen Hardware und behält so einfacher die Kontrolle über seine Daten und Prozesse. Diese Möglichkeit wird aber durch den Hersteller zukünftig weniger angeboten.

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.

Für Smartphones und Tablets mit dem Betriebssystem Android steht ab der Version 5 (Lollipop) eine Geräteverschlüsselung zur Verfügung (zu finden unter Sicherheitseinstellungen). Hierbei wird vom Betriebssystem der gesamte Datenspeicher des Gerätes verschlüsselt. Der Speicher kann dann ohne den Sperrcode, der gleichzeitig als Gerätesperre und Bildschirmsperre dient, nicht von Unbefugten ausgelesen werden, falls das Gerät verloren geht.

Bei Smartphones und Tablets mit dem Betriebssystem iOS der Firma Apple existiert die Geräteverschlüsselung ab der Version 7. Damit die Verschlüsselung zum Tragen kommt, muss ebenfalls eine sogenannte Code-Sperre eingerichtet werden. Dadurch wird wie bei Android bei jedem Einschaltvorgang des Gerätes ein Passwort abgefragt.

Im Übrigen ermöglicht die bloße SIM-Sperre keinen Schutz vor unbefugten Zugriff auf den Speicher und die Daten, sondern verhindert nur, dass die SIM-Karte für Telefonate genutzt werden kann.

Auch bei Laptops ist eine komplette Geräteverschlüsselung möglich. Im Betriebssystem Windows (bei Version 8 und 10 in der Ausführung Professional und Enterprise) kann die Festplatte mit Hilfe des integrierten BitLockers (zu finden unter Geräteverschlüsselung in den Einstellungen) verschlüsselt werden. Bei Laptops der Firma Apple ist dies mit dem integrierten FileVault ab MacOS X Lion in den Systemeinstellungen im Menüpunkt „Sicherheit“ möglich. Steht keine integrierte Verschlüsselungsmethode zur Verfügung, kann das freie und quelloffene VeraCrypt z. B. auf Linux-Geräten oder in Windows Home-Umgebungen eine Verschlüsselung ermöglichen. Bei VeraCrypt ist neben der Verschlüsselung der gesamten Betriebssystem-Festplatte auch die Verschlüsselung eines Datei-Containers möglich. Hierbei wird ein zuvor definierter Speicherbereich verschlüsselt, in welchem dann die zu schützenden Daten abgelegt werden können.

Bei externen Festplatten und USB-Sticks können ebenfalls BitLocker oder VeraCrypt angewendet werden, indem jeweils das gesamte Medium verschlüsselt oder ein verschlüsselter Container darauf angelegt wird. Im Übrigen sind auf dem IT-Markt auch Lösungen mit integrierter Hardware-basierter Verschlüsselung erhältlich, so z. B. mobile Festplatten und USB-Sticks mit Zifferntastatur zur PIN-Eingabe.

Hilfsweise können zu transportierende Dateien auch vorab (z. B. bei CDs und DVDs) in ZIP-Archiven verschlüsselt werden. Dabei muss über ein Archivierungsprogramm, wie z. B. WinZIP, 7-Zip, WinRAR o. ä., ein Passwort für das zu erstellende Archiv vergeben werden, wonach dieses automatisch verschlüsselt erstellt wird. Auch Büro-Software-Produkte wie Microsoft Office, Libre Office oder Adobe Acrobat unterstützen die passwortgeschützte Speicherung einzelner Dokumente.

Bei allen Verschlüsselungsverfahren, die ein Passwort bzw. einen Sperrcode benötigen, gilt: Je länger und komplexer das Passwort, desto sicherer die Verschlüsselung.

Der Landesbeauftragte hat zum Datenträgerschutz eine Handreichung entwickelt, die auch auf seiner Homepage veröffentlicht wurde[10].

6.10 SPAM-Schutz im Landesnetz verbessern

SPAM-E-Mails oder Junk-E-Mails sind elektronische Mitteilungen, die beim Empfänger unverlangt und unerwünscht eingehen und das Postfach – im besten Fall nur mit Werbung, meist aber mit Schadsoftware oder Verweisen auf solche – füllen. Im aktuellen Berichtszeitraum wurden wiederholt Schäden durch SPAM-E-Mails, insbesondere durch nachgeladene Verschlüsselungstrojaner („Emotet“), gemeldet. Unter anderem wurde das Ministerium für Justiz und Gleichstellung, wie auch verschiedene Unternehmen im Land, angegriffen.

Die beste Vorsorge gegen Datenverluste sind zeitnah erstellte oder aktualisierte Sicherungskopien (Backups). Es wird generell davon abgeraten, Lösegeldforderungen nachzugeben. Mit etwas Glück hilft es, auf eine Entschlüsselungssoftware Dritter zu warten.

Auch im Landesnetz wird zunehmend mehr SPAM festgestellt. Die E-Mail-Server des Landesnetzes filtern und markieren bereits jetzt mit hohem Aufwand und nicht immer 100%iger Erkennungsrate solche E-Mails. Es werden täglich, u. a. durch das CERT Nord, Listen mit Webservern, von denen aus SPAM-Mails ausgehen, aktualisiert und verschlüsselt verteilt. Nur leider war es bis dato nicht möglich, die Adressen solcher Server zentral sperren zu lassen. Jede Behörde soll sich stattdessen selbst um die Sperre kümmern, was zum Scheitern verurteilt ist, solange dies nicht automatisiert zeitnah durchgeführt werden kann. Hier besteht erheblicher Verbesserungsbedarf. Das Ministerium der Finanzen bemüht sich darum.

Dabei reicht es nicht aus, nur filter- und softwarebasiert SPAM zu suchen. Es sollte vielmehr auch aktiv bei der Bekämpfung von SPAM geholfen werden. Dazu gibt es die Standards SPF, DKIM und DMARC.

SPF steht für Sender Policy Framework und bedeutet nichts anderes, als dass in den veröffentlichten Einträgen im Domain Name System (DNS) zu einer Internet-Domain vermerkt wird, welche E-Mail-Server berechtigt sind, E-Mails für diese Domains zu versenden. Eine ähnliche Überprüfung findet bereits auf den E-Mail-Servern des Landes statt, um unerwünschte E-Mails (Absender mit Landes-Adresse, aber vom Internet kommend) abweisen zu können. SPF erlaubt es nun auch dem Empfänger

[10] https://lsaurl.de/Datentraegerschutz.

einer E-Mail zu prüfen, ob die E-Mail von einem erlaubten E-Mail-Server verschickt und somit berechtigt versandt wurde.

Mittels DomainKeys Identified Mail (DKIM) können E-Mails durch den E-Mail-Server automatisiert digital signiert werden. Eine solche Signatur kann vom empfangenden Server unter Hinzuziehung von im DNS hinterlegten kryptografischen Schlüsseln geprüft werden. Damit steht fest, dass die E-Mail vom zur Internet-Domain gehörenden Server verschickt und unterwegs auch nicht verändert wurde. Diese Informationen lassen sich zur Filterung ankommender E-Mails nutzen.

Auch Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzt das DNS, um Informationen zu hinterlegen. Hier kann der Absender ergänzende Hinweise geben, wie der Empfänger die E-Mail – insbesondere hinsichtlich Abweichungen bei SPF und DKIM – behandeln soll. So lässt sich regeln, wann E-Mails als SPAM markiert, gemeldet oder verworfen werden sollen.

Der Landesbeauftragte regt an, auf den E-Mail-Servern des Landes SPF, DKIM und DMARC im DNS zu aktivieren. Das hilft aktiv bei der SPAM-Bekämpfung. Auch soll das Ministerium der Finanzen die zentrale Proxy-Sperre rasch umsetzen. Damit könnten alle Ressorts im Land mit einer Aktion wirksam geschützt werden.

6.11 Prüfung des Zentralen Meldedatenbestandes bei Dataport

Im März 2017 startete ein komplexes Prüfvorhaben des von Dataport betriebenen Fachverfahrens Zentraler Meldedatenbestand (s. XIII./XIV. Tätigkeitsbericht Nr. 4.6). Da dieses Verfahren, welches dem automatisierten Meldedatenabruf gemäß Bundesmeldegesetz (BMG) dient, von den Innenressorts der Dataportträgerländer Hamburg, Schleswig-Holstein und Sachsen-Anhalt in einer gemeinsamen Basisinfrastruktur bei Dataport beauftragt wird, wurde die Prüfung des Verfahrens durch die Datenschutzaufsichtsbehörden der o. g. Länder in gemeinsamer Abstimmung durchgeführt.

Die Prüfung sollte zunächst hauptsächlich die technische und organisatorische Umsetzung des Verfahrens in den Blick nehmen. Dazu wurde ein mehrtägiger Vor-Ort-Termin bei Dataport mit Vertretern der wichtigsten Kernbereiche (Verfahrensmanagement, Administration, IT-Sicherheit, Datenschutz) durchgeführt. Nachdem ein Sachstandsbericht erstellt und Stellungnahmen eingeholt wurden, begann eine umfangreiche Dokumentations-Prüfung. Dazu musste eine nicht unbedeutende Anzahl an Dokumenten nachgefordert und auf eine Aktualisierung von wichtigen Dokumentationen auch hinsichtlich Anpassungen an die DS-GVO hingewirkt werden. Seitens Dataport wurden viele während dieser Prüfphase und bereits vorab festgestellte Mängel fortlaufend behoben.

Jedoch sind im Laufe der Prüfung auch rechtliche Fragestellungen in den Fokus getreten. So wurde u. a. festgestellt, dass die Art und Weise, wie die Verantwortlichen die Zwecke und Mittel zur Verarbeitung gemeinsam festlegen, den Bestimmungen des Art. 26 DS-GVO unterliegt. Daher muss eine Vereinbarung gem. Art. 26 Abs. 1 DS-GVO zwischen den Innenressorts der Auftraggeberländer getroffen werden.

Dies wurde mit den Innenressorts in einer gemeinsamen Beratung im September 2019 im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt erörtert. Im Dezember 2019 legte das Ministerium für Inneres und Sport einen abgestimmten Entwurf zu einer Vereinbarung gem. Art. 26 Abs. 1 Satz 1 DS-GVO zwischen den Innenressorts der Auftraggeberländer zum Zentralen Meldedatenbestand bei Dataport vor; dieser wird noch von den Datenschutzaufsichtsbehörden kommentiert.

Außerdem ist im Verlauf der Prüfung aufgefallen, dass die Protokollierung automatisierter Datenabrufe von in § 34 Abs. 4 Satz 1 BMG genannten Stellen (Strafverfolgungs- und Sicherheitsbehörden) von den Innenressorts bei Dataport beauftragt und innerhalb des Verfahrens umgesetzt wurde, obwohl § 40 Abs. 3 BMG vorschreibt, dass die Protokollierung durch diese abrufenden Stellen selbst zu erfolgen hat. Eine Auflösung dieses Widerspruchs ist noch Gegenstand der Erörterungen.

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 Löschungsgebot (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. Löschungsregelungen:

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 Löschungsinteresse 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 übli-

chen 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

7.1 Webtracking – Orientierungshilfe für Anbieter von Telemedien

Die DSK veröffentlichte am 26. April 2018 eine vorläufige Positionsbestimmung zur Anwendbarkeit des Telemediengesetzes für nichtöffentliche Stellen ab dem 25. Mai 2018. Hintergrund war die ausstehende E-Privacy-Verordnung. In der Positionsbestimmung wurden insbesondere Fragen der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen erörtert. Gleichzeitig beschlossen die Datenschutzaufsichtsbehörden, eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen durchzuführen (vgl. XV. Tätigkeitsbericht, Nr. 6.1).

Als Ergebnis der Auswertung der Stellungnahmen im Konsultationsverfahren und zur Erläuterung und Konkretisierung der Positionsbestimmung haben die Datenschutzaufsichtsbehörden im März 2019 eine Orientierungshilfe für Anbieter von Telemedien herausgegeben[11], die allerdings unter dem ausdrücklichen Vorbehalt eines zukünftigen – möglicherweise abweichenden – Verständnisses der maßgeblichen Vorschriften durch den EDSA sowie einer etwaigen Rechtsänderung durch ein Inkrafttreten einer Überarbeitung der Richtlinie 2002/58/EG steht.

Diese Orientierungshilfe soll der Umsetzung der datenschutzrechtlichen Anforderungen an die Verarbeitung der Daten von Nutzerinnen und Nutzern durch Telemediendienste dienen. Dabei wird den Verantwortlichen anhand von Beispielen aufgezeigt, dass die Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse) eine Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Nutzerinnen und Nutzer verlangt und auf den konkreten Einzelfall bezogen sein muss. Insbesondere bei der webseitenübergreifenden Nachverfolgung des Nutzerverhaltens und der Weitergabe von Nutzerdaten an Dritte, die diese Daten zu eigenen Zwecken verarbeiten, fällt die Interessenabwägung zugunsten des Betroffenen aus. Das heißt, dass als Rechtsgrundlage Art. 6 Abs. 1 lit. f DS-GVO nicht in Betracht kommt, sondern eine informierte Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO erforderlich ist.

Mitte November 2019 veröffentlichten die Datenschutzaufsichtsbehörden in einer abgestimmten Aktion zusätzlich jeweils eigene Mitteilungen zum Einsatz von Google Analytics und ähnlichen Analysediensten. Darin wurde unter Hinweis auf die Orientierungshilfe noch einmal Folgendes verdeutlicht: Werden in Webseiten Dritt-Dienste wie z. B. Google Analytics eingebunden, deren Anbieter in der Standardkonfiguration personenbezogene Daten auch für eigene Zwecke nutzen, ist das rechtlich nur zulässig, wenn vorher eine ausdrückliche Einwilligung der Nutzerinnen und Nutzer eingeholt wird. Hierzu ist ein zusammenfassendes Papier der DSK in Vorbereitung.

[11] https://lsaurl.de/OHTelemedien

Zudem ist ein sogenannter Cookie-Banner unzureichend, der das Weitersurfen auf der Webseite als Einwilligung deklariert. Dasselbe gilt für voraktivierte Kästchen bei Einwilligungserklärungen. Dies wurde auch durch das Urteil des Europäischen Gerichtshofs vom 1. Oktober 2019 (Az. C-673/17, „Planet49“) bestätigt.

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 Entschließung 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 ordnungsgemäßen 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**). 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.

7.3 Sprachassistenzsysteme

Bei der Nutzung von Sprachassistenzsystemen wie Amazons Alexa, Apples Siri oder dem Google Assistant wurden seit Jahren Mitschnitte angefertigt. Diese wurden von deren Mitarbeitern bzw. beauftragten Firmen mit dem Ziel ausgewertet, die Qualität der Spracherkennung zu verbessern. Dabei geht es zum Beispiel um Fälle, in denen Sprachassistenten nicht richtig reagierten, um die falsche Erkennung von Aktivierungswörtern oder um für das System unbekannte Sprachen und Dialekte.

Die fehlerhaften Aktivierungen, bei denen die Software nämlich die Aktivierungswörter unzutreffend erkannt hat, sind ein besonderes Problem. Denn dabei können Sätze und Unterhaltungen aufgezeichnet werden, die gar nicht an den Sprachassistenten gerichtet waren. Medienberichten zufolge waren in den Mitschnitten auch sehr private Details zu hören, wie z. B. medizinische, geschäftliche oder intime Inhalte.

Problematisch ist insbesondere, dass den meisten Nutzern solcher Sprachassistenzsysteme diese Praxis nicht bewusst war – also datenschutzrechtlich ohne Einwilligung erfolgte – und sie erst durch die Medien darüber informiert wurden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit eröffnete vor diesem Hintergrund Ende Juli 2019 ein Verwaltungsverfahren, um Google zu untersagen, entsprechende Auswertungen durch Mitarbeiter oder Dritte für den Zeitraum von drei Monaten vorzunehmen. Damit sollten die Persönlichkeitsrechte der Betroffenen zunächst vorläufig geschützt werden, da erhebliche Zweifel bestanden, dass der Einsatz des Google Assistant die Vorgaben der DS-GVO erfüllt. Zwar ist die für Google zuständige Behörde die irische Datenschutzaufsichtsbehörde, da sich die Hauptniederlassung von Google in Irland befindet. Allerdings sieht Art. 66 Abs. 1 DS-GVO für Datenschutzbehörden in anderen Mitgliedstaaten auch die Möglichkeit vor, für einen Zeitraum von höchstens drei Monaten Maßnahmen in ihrem Zuständigkeitsbereich zu treffen, wenn ein dringender Handlungsbedarf zum Schutz von Rechten und Freiheiten Betroffener besteht.

Mittlerweile lassen Google und Apple solche Auswertungen nur noch nach ausdrücklicher Einwilligung der Nutzer vornehmen. Amazon bietet dem Nutzer lediglich die Möglichkeit, einer solchen Auswertung zu widersprechen.

7.4 Änderung des Rundfunkbeitragsstaatsvertrages – Meldedatenabgleich

Im Oktober 2019 wurde von den Regierungschefinnen und Regierungschefs der Länder der Dreiundzwanzigste Rundfunkänderungsstaatsvertrag (RÄStV) unterzeichnet. In Artikel 1 RÄStV wird der Rundfunkbeitragsstaatsvertrag unter anderem dahingehend geändert, dass ein regelmäßiger Meldedatenabgleich stattfindet: Beginnend mit dem Jahr 2022 werden alle vier Jahre die Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt übermittelt.

In ihrem Beschluss vom 26. April 2019 hat die DSK gefordert, den regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen (**Anlage 10**). Die im Beschluss aufgeführten Bedenken wurden durch einen Vertreter der DSK in der nichtöffentlichen mündlichen Anhörung der Rundfunkkommission der Länder am 29. April 2019 vertreten.

Der Dreiundzwanzigste Rundfunkänderungsstaatsvertrag wurde von den Regierungschefinnen und Regierungschefs der Länder jedoch unverändert beschlossen und bedurfte sodann der Ratifizierung durch die Länderparlamente. Zum entsprechenden Gesetzentwurf für Sachsen-Anhalt (LT-Drs. 7/5321) wurde der Landesbeauftragte trotz der datenschutzrechtlichen Relevanz weder von der Landesregierung noch vom Landtag beteiligt.

Die Landesregierung hatte die Datenschutzrelevanz des Meldedatenabgleichs verkannt, denn im Gesetzentwurf wurde das Zitiergebot gem. Art. 19 Abs. 1 Satz 2 GG nicht beachtet. Eine Ergänzung erfolgte erst mittels der Beschlussempfehlung des Ausschusses für Bundes- und Europaangelegenheiten sowie Medien (vgl. LT-Drs. 7/5740). Das Ratifizierungsgesetz ist am 21. März 2020 in Kraft getreten (GVBl. LSA S. 81).

8 Öffentliche Sicherheit

8.1 SOG LSA – Zuverlässigkeitsüberprüfung

Mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Nr. 4.1.2) wurden auch einige Neuerungen in das SOG LSA eingeführt. Der Landesbeauftragte hatte das Ministerium für Inneres und Sport zu dem Gesetzentwurf beraten und auch gegenüber dem Landtag Stellung genommen.

Einer von mehreren kritisierten Punkten war eine Regelung, nach der im Informationssystem der Polizei des Landes Sachsen-Anhalt gespeicherte Daten oder im polizeilichen Informationsverbund zwischen Bund und Ländern zum Abruf durch die Polizei bereitstehende Daten zum Zwecke der Durchführung einer Zuverlässigkeitsüberprüfung für Einstellungen in den Polizeivollzugsdienst weiterverarbeitet werden können. Gegen die Validität des Datenbestandes bestehen jedoch Bedenken. Werden den Sachverhalt nicht vollständig wiedergebende Informationen für die Durchführung solcher Zuverlässigkeitsüberprüfungen verwendet, kann dies gravierende Folgen für die Betroffenen haben. Die bekannte Abwägung zwischen im Einzelfall berechtigten und schutzwürdigen Interessen des Dienstherrn und den schutzwürdigen Interessen der Bewerber (Persönlichkeitsrecht, Grundrecht auf informationelle Selbstbestimmung) ist in Frage gestellt. So hat beispielsweise das Bundesarbeitsgericht in einem den öffentlichen Dienst betreffenden Verfahren am 15. November 2012 (Az.: 6 AZR 339/11) unter Hinweis auf die Wertordnung des Grundgesetzes entschieden, dass für den Dienstherrn grundsätzlich kein berechtigtes Interesse an der unspezifischen Frage nach eingestellten Ermittlungsverfahren besteht.

Nach Auffassung des Landesbeauftragten ist eine Berücksichtigung von nur bedingt belastbaren Polizeiinformationen auch nicht mit den entgegenstehenden Maßgaben des Bundesrechts im Bundeszentralregistergesetz vereinbar. Danach stehen für Einstellungsverfahren, auch im öffentlichen Dienst, grundsätzlich Führungszeugnisse zur Verfügung. Dies impliziert die Wertung, dass alle die Verurteilungen, Schuldsprüche oder Verwarnungen mit Strafvorbehalt und natürlich erst recht bloße Informationen, die nicht nach § 41 BZRG aufgenommen werden, dem Betroffenen im Rechtsverkehr gerade nicht entgegengehalten werden dürfen. Abfragen von Informationen der genannten Systeme sind daher auch als Umgehung der §§ 41, 43 BZRG anzusehen.

Im Ergebnis blieb es jedoch bei der fragwürdigen Regelung (§ 29 SOG LSA).

8.2 Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung

Trägerländer des Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ) sind Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen. Aufgabe des GKDZ ist es, länderübergreifend, insbesondere im Wege der Auftragsverarbeitung mit spezifischen IT-Leistungen, die Telekommunikationsüberwachung zu unterstützen. Ziel ist es, die als Anstalt des öffentlichen Rechts im Januar 2018

eingerichtete Institution bis Ende 2021 arbeitsfähig zu machen, d. h. in den sog. Wirkbetrieb gehen zu lassen.

Der Landesbeauftragte hatte in der Vergangenheit sowohl zu dem der Gründung des GKDZ zugrundeliegenden Staatsvertrag Stellung genommen (s. XIII./XIV. Tätigkeitsbericht, Nr. 6.6) als auch bei der Beratung des GKDZ in der bisherigen Aufbauphase mitgewirkt (s. XV. Tätigkeitsbericht, Nr. 7.2).

Im Berichtszeitraum hat der Landesbeauftragte in Zusammenarbeit mit den Landesbeauftragten der anderen Trägerländer die Planungen des GKDZ weiter begleitet. Das GKDZ hat im Berichtsjahr ein Konzept für die technische und organisatorische Feinplanung vorgelegt. Hierzu fanden im Februar und Oktober 2019 Besprechungen mit dem GKDZ statt. In Rahmen der zweiten Besprechung wurden auch die Räumlichkeiten in Leipzig besichtigt. Im Anschluss wurde dem GKDZ eine gemeinsame Stellungnahme zum Feinkonzept durch die Landesbeauftragten der Trägerländer übersandt.

Der Landesbeauftragte wird auch die weiteren Ausbaustufen des GKDZ in Zusammenarbeit mit den Aufsichtsbehörden der anderen Trägerländer datenschutzrechtlich begleiten.

8.3 „Polizei 2020“

Im November 2016 verständigten sich die Innenminister des Bundes und der Länder auf die Saarbrücker Agenda zur Informationsarchitektur der Polizeien des Bundes und der Länder als Teil der Inneren Sicherheit. Mit dem Programm „Polizei 2020“ will der Bund einen Beitrag zur Umsetzung der Saarbrücker Agenda leisten, indem das Informationswesen der Polizeien des Bundes und der Länder vereinheitlicht und harmonisiert werden soll. Handlungsleitend sei dabei der polizeifachliche Bedarf. Ziel sei es, der Polizei nach Maßgabe der Gesetze und unter Berücksichtigung des Datenschutzes zu jeder Zeit an jedem Ort die für die polizeiliche Arbeit erforderlichen Daten zur Verfügung zu stellen. So wird es zumindest im „White Paper“ zum Projekt „Polizei 2020“ des Bundesinnenministeriums ausgeführt.

Tatsächlich belastbare Erkenntnisse zum Projekt „Polizei 2020“ liegen dem Landesbeauftragten bisher kaum vor. Insbesondere die Auswirkungen auf die Datenverarbeitung durch die Polizei des Landes Sachsen-Anhalt können derzeit noch nicht eingeschätzt werden. Offenbar sollen die bisherigen Verbunddateien des bundesweiten polizeilichen Informationssystems abgeschafft und durch ein neues „Datenhaus“ im Rahmen des Projekts „Polizei 2020“ ersetzt werden.

Die rechtlichen Grundlagen für diesen neuen Informationsverbund finden sich im Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten. Deren Anwendung auf das Projekt „Polizei 2020“ bedarf einer eingehenden datenschutzrechtlichen Bewertung, - etwa im Hinblick auf das Prinzip der Zwecktrennung -, die zunächst dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit obliegt. Der Landesbeauftragte wird das Projekt auf Landesebene in den sich auf die Landespolizei des Landes Sachsen-Anhalt auswirkenden Aspekten begleiten.

9 Verfassungsschutz

Im August 2019 gab die Landesregierung den Entwurf eines Gesetzes zur Fortentwicklung des Verfassungsschutzes und der Sicherheitsüberprüfung zur Anhörung frei. Mit diesem Gesetzentwurf sollte der im Jahr 2012 begonnene Reformprozess im Verfassungsschutz fortgeführt werden. Sowohl die Empfehlungen aus dem NSU-Untersuchungsausschuss des Bundestages (BT-Drs. 17/14600) als auch das Urteil des Bundesverfassungsgerichts vom 24. April 2013 (1 BvR 1215/07), welches sich u. a. mit dem informationellen Trennungsprinzip zwischen den Nachrichtendiensten und der Polizei befasst, sollten in der Novellierung ihren Niederschlag finden. Des Weiteren sollte auch auf die grundlegenden Veränderungen der Kommunikationswege und elektronischen und digitalen Kommunikationsmittel reagiert und es sollten die nachrichtendienstlichen Befugnisse erweitert werden.

Der Landesbeauftragte hatte bereits im Februar 2019 eine erste Stellungnahme zu einem Vorentwurf des Ministeriums für Inneres und Sport abgegeben. In der Stellungnahme im Rahmen der o. a. Anhörung wurden, soweit den Änderungsvorschlägen der ersten Stellungnahme nicht gefolgt worden war, die Kritikpunkte aufrechterhalten und ergänzt. Diese betrafen zum einen die nicht vorhandene oder unzureichende Begründung der Regelungen des Gesetzes sowie die Nichtbeachtung des Zitiergebotes bei Grundrechtseingriffen. Zum anderen wurden inhaltlich u. a. die Regelungen zur Überwachung der Telekommunikation, zur Speicherung, Veränderung und Nutzung personenbezogener Daten von Minderjährigen und zur Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörde kritisch bewertet.

Das geltende Verfassungsschutzgesetz enthält in § 30 eine Verweisung auf Regelungen des DSG LSA. Bereits im Berichtszeitraum war absehbar, dass dieses außer Kraft treten und vom neuen DSAG LSA abgelöst werden sollte. Das ist dann auch im Februar 2020 erfolgt (GVBl. LSA 2020 S. 25). Vor diesem Hintergrund sollten im Rahmen der Novellierung des Verfassungsschutzgesetzes auch datenschutzrechtliche Regelungen im Gesetz selbst aufgenommen werden. Das würde nicht nur die Problematik der Verweisung auf ein außer Kraft getretenes Gesetz vermeiden, sondern auch der Rechtsklarheit und Nutzerfreundlichkeit dienen.

Der Gesetzentwurf wurde von der Landesregierung im Januar 2020 beschlossen und liegt dem Landtag vor (LT-Drs. 7/5612). Die vom Landesbeauftragten kritisierte Regelung zur Quellen-TKÜ bzw. für Eingriffe in informationstechnische Systeme ist nicht mehr Gegenstand des Entwurfes.

10 Rechtspflege und Justizvollzug

10.1 Datenschutz im Justizvollzug

Im XV. Tätigkeitsbericht (vgl. Nr. 9.1) hatte der Landesbeauftragte darauf hingewiesen, dass der Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung der Datenschutzvorschriften im Bereich des Justizvollzuges von Sachsen-Anhalt (Justizvollzugsdatenschutzumsetzungsgesetz Sachsen-Anhalt) u.a. wegen der unübersichtlichen Gesetzessystematik, der europarechtswidrigen Einschränkung der bereits bestehenden Kontrollkompetenzen des Landesbeauftragten,

der Einräumung präventiv-polizeilicher Befugnisse zur Abwehr drohender Gefahren und der weitreichenden Regelung zur Überprüfung anstaltsfremder Personen, insbesondere von Besuchern, durch den Verfassungsschutz kritisch zu sehen sei.

Der Landesbeauftragte hat sich vertieft mit der Problematik befasst, ob eine datenschutzkonforme Regelung der Überprüfung von Gefangenen und anstaltsfremden Personen im Strafvollzug bei „drohender Gefahr“ (s. den Entwurf der Landesregierung vom Januar 2019 in LT-Drs. 7/3858) möglich wäre.

Der Begriff der „drohenden Gefahr“ orientiert sich an der Rechtsprechung des Bundesverfassungsgerichts zu Regelungen der Terrorismusabwehr (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 1-29) und bezeichnet das Vorfeld einer konkreten, unmittelbar bevorstehenden oder gegenwärtigen Gefahr.

In den §§ 24 bis 25 des Entwurfes des Justizvollzugsdatenschutzumsetzungsgesetzes finden sich die vom Bundesverfassungsgericht genannten Kriterien nicht wieder. Die Normen knüpfen nicht an das Vorliegen einer terroristischen Gefahr für ein überragend wichtiges Rechtsgut an, sondern machen jegliche drohende Gefahr schon im Vorfeld einer konkreten Gefahrenlage für die Sicherheit der Anstalt zur Eingriffsvoraussetzung. Die Eingriffsschwelle ist eher niedrig, denn das Merkmal ist auch erfüllt bei Verstößen eines Gefangenen, die man eher als Bagatellverstöße einstufen würde, so z. B. beim unerlaubten Besitz einer Spielkonsole oder eines CD-Players.

Nach dem Wortlaut der Norm wären die Voraussetzungen für eine Überprüfung durch den Verfassungsschutz bereits dann gegeben, wenn Anhaltspunkte dafür bestehen, dass ein Gefangener sich die o. g. Gegenstände zu verschaffen versucht bzw. wenn Anhaltspunkte bestehen, dass Besucher diese Gegenstände, z. B. als Geschenk, mitbringen werden. Hinweise, dass schwere Straftaten, insbesondere im terroristischen oder extremistischen Bereich begangen werden könnten, müssen nicht bestehen. Hinzu kommt, dass der Ort der Tatbegehung bei einer Justizvollzugsanstalt anders als im Terrorismusbereich vorhersehbar ist.

Der Landesbeauftragte hat im Rahmen seiner Stellungnahmen darauf hingewiesen, dass eine Überprüfung des o. g. Personenkreises durch den Verfassungsschutz bei Vorliegen einer drohenden Gefahr für die Sicherheit der Anstalt daher unverhältnismäßig sei, da der Eingriff nahezu grenzenlos möglich werde. Eine Einwilligung des Besuchers in seine Überprüfung durch den Verfassungsschutz komme im Übrigen nicht in Betracht, da die Einwilligung nicht freiwillig sei; erteile er sie nämlich nicht, dürfe er den Gefangenen nicht besuchen.

Der Landesbeauftragte hat daher empfohlen, auf die geplanten Regelungen entweder ganz zu verzichten oder die Eingriffsschwelle für eine Überprüfung deutlich zu erhöhen.

Die Beratungen im Landtag zum Regierungsentwurf dauern zum Redaktionsschluss noch an.

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 e^2-Software-Suite wurde mit dem Aufbau des Backend-Betriebes für die e^2-Pilotierung im Rechenzentrum (RZ^2) 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 (MBl. LSA 2019, S. 169). Die Einrichtung der Behördenpostfächer hat begonnen.

10.3 Automatisierte Kennzeichenerfassungssysteme

Die Polizei setzt in mehreren Bundesländern automatisierte Kennzeichenerfassungssysteme ein. Dies geschieht grundsätzlich zum Zwecke der Gefahrenabwehr, wird aber vereinzelt auch für die Strafverfolgung genutzt. Es hat sich gezeigt, dass zumindest in Brandenburg die Technik schon jetzt dazu verwandt wird, nicht nur nach bestimmten Kennzeichen zu suchen, sondern sie auch im sog. Aufzeichnungsverfahren für strafrechtliche Ermittlungsverfahren zu nutzen. Dies hat zur Folge, dass über einen längeren Zeitraum die Kennzeichen sämtlicher Kraftfahrzeuge, die die Erfassungsstellen passieren, eingelesen und langfristig gespeichert werden.

Vor diesem Hintergrund hat sich die DSK mit einer Entschließung vom 6. November 2019 gegen die massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke gewandt (**Anlage 9**). Kern der Kritik der DSK ist die massenhafte und teilweise längerfristige Erfassung von Kfz-Daten unabhängig von der Beschuldigteneigenschaft der Betroffenen. Für diese exzessive Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung gibt es auch keine Rechtsgrundlage, so dass neben der Unterlassung dieser Praxis auch die Löschung der rechtswidrig gespeicherten Daten gefordert wurde.

11 Forschung, Hochschulen und Schulen

11.1 Forschung

11.1.1 Forschungsprojekte

Im Berichtszeitraum wurde der Landesbeauftragte bei einigen neuen Forschungsprojekten im Bildungs- und Medizinbereich beteiligt. Überdies erfolgte bei mehreren Bildungsstudien im Schulbereich eine erneute datenschutzrechtliche Begleitung der jährlichen Erhebungswellen.

Einen Schwerpunkt der datenschutzrechtlichen Prüfung nahm aufgrund der Komplexität des Gesamtprojektes im Berichtszeitraum das Projekt „Leistung macht Schule/LemaS“ ein. Hierbei handelt es sich um eine Förderinitiative von Bund und Ländern mit dem Ziel, die Entwicklungsmöglichkeiten von potentiell besonders leistungsfähigen Schülern im Regelunterricht zu optimieren. Die Umsetzung erfolgt in 22 Teilprojekten. Es wurden insgesamt zehn Teilprojekte zur datenschutzrechtlichen Prüfung vorgelegt. Diesbezüglich hat der Landesbeauftragte u. a. Hinweise zu den Einwilligungserklärungen der Eltern und Lehrkräfte, der erforderlichen Informationen an die Eltern hinsichtlich der Datenverarbeitung im Rahmen der Videografie und der Speicherdauer der personenbezogenen Daten gegeben.

11.1.2 Reichweite der Einwilligung (Broad Consent)

Nach Art. 4 Nr. 11 DS-GVO ist eine Einwilligung stets für den „bestimmten Fall“, in informierter Weise und unmissverständlich abzugeben. Das Erfordernis des „bestimmten Falls“ konkretisiert den Grundsatz der Zweckbindung im Sinne des Art. 5 Abs. 1 lit. b DS-GVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke zu verarbeiten sind.

Diese strengen Regelungen sind eine Grenze für Forschungsanliegen, insbesondere im medizinischen Bereich. Die Tendenz geht zunehmend dahin, große Mengen von Daten aus der Krankenversorgung zu sammeln. Sie sollen für Forschungen zu Zwecken besserer medizinischer Versorgung in Kooperation mit anderen Forschungseinrichtungen und Industriepartnern im Rahmen einer IT-Architektur für die interoperable Nutzung zur Verfügung gestellt werden (vgl. Nr. 11.1.3). Bei großen Forschungsprojekten wird zumindest gefordert, die für den Forschungszweck erhobenen Daten auch für künftig sich erst aus den Projekten ergebende neue Projekte bzw. Forschungsfragen nutzen zu können.

Hierzu beruft man sich auf die vielfache Privilegierung der Forschung in der DS-GVO und insbesondere auf ErwGr 33. Wenn der Zweck der Verarbeitung für Zwecke wissenschaftlicher Forschung zum Zeitpunkt der Erhebung nicht vollständig angegeben werden kann, soll erlaubt sein, die Einwilligung „für bestimmte Bereiche wissenschaftlicher Forschung“ zu geben. Es ist daher die Frage zu beantworten, wieviel Spielraum im Rahmen der Vorgabe der verbindlichen Zweckbestimmung bei der Einwilligung gegeben ist.

Hierzu haben sich die Datenschutzaufsichtsbehörden des Bundes und der Länder mit Vertretern der Forschung, insbesondere der Telematikplattform für Medizinische Forschungsnetze, beraten. Die Datenschutzaufsichtsbehörden haben dazu am

3. April 2019 einen Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO gefasst.[12] Danach können ausnahmsweise bei der einer Datenerhebung zeitlich vorgelagerten Einwilligung unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden (broad consent). Das Gebot einer informierten Einwilligung erfordert aber zumindest, dass möglichst präzise das jeweilige Forschungsvorhaben transparent gemacht wird und bestimmte spezifische Sicherungsmaßnahmen ergriffen werden. Die notwendigen Kompensationsmaßnahmen für die Unschärfe der Zweckbestimmung sind in dem Beschluss aufgeführt.

11.1.3 Medizininformatik-Initiative

Die vom Bundesministerium für Bildung und Forschung geförderte Medizininformatik-Initiative (MII) hat die Verbesserung von Forschungsmöglichkeiten und Patientenversorgung durch IT-Lösungen im Rahmen einer zentralen Forschungsinfrastruktur zum Ziel. Künftig sollen ein standortübergreifender Austausch und die Nutzung von Daten aus der Krankenversorgung für klinische und biomedizinische Forschung erfolgen. Gefördert werden Konsortien, zu denen sich jeweils mehrere Universitätskliniken mit weiteren Partnern (Forschungsinstitute, Hochschulen, Unternehmen, Krankenhäuser) zusammengeschlossen haben.

In Sachsen-Anhalt sind die Universität und das Universitätsklinikum in Magdeburg und das Universitätsklinikum in Halle jeweils in einem der Konsortien beteiligt. In Magdeburg und in Halle werden in den Einrichtungen zunächst sogenannte Datenintegrationszentren eingerichtet, die die Daten aus der Krankenversorgung auf Einwilligungsbasis erhalten und für die Nutzbarkeit für auch einrichtungsübergreifende Forschungszwecke aufbereiten. Der Landesbeauftragte hat sowohl in Halle als auch in Magdeburg bereits Beratungen mit den Einrichtungen durchgeführt und wird die Projekte auch weiter datenschutzrechtlich begleiten.

Der gemeinsame Entwurf einer Einwilligungserklärung für alle MII-Konsortien wurde mit der DSK umfänglich erörtert. Dabei wurden Optimierungen in Bezug auf Konkretisierungsbedarf, Transparenz, Darstellung der Risiken und den Umgang mit Bioproben erreicht.

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

[12] https://lsaurl.de/dskwissfo

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.

11.2.2 Medienkompetenz

Die Landesarbeitsgemeinschaft „Medienbildung/Medienkompetenz“ hat im Berichtszeitraum zweimal getagt. Der Landesbeauftragte nahm an den Sitzungen teil und setzte sich wie in der Vergangenheit dafür ein, dass der Informationsaustausch innerhalb der Arbeitsgemeinschaft im Sinne des Netzwerkgedankens verstärkt wird.

Für das Landesbildungsministerium stand und steht die Umsetzung des Digitalpaktes im Mittelpunkt der Arbeit (s. Nr. 11.2.1). Eine Voraussetzung für die Beantragung von Mitteln aus dem Digitalpakt ist die Vorlage eines technisch-pädagogischen Konzeptes jeder Schule. Zur Unterstützung bei der Erarbeitung eines neuen oder Überarbeitung des bereits bestehenden Medienbildungskonzeptes hat das Landesinstitut für Schulqualität und Lehrerbildung Sachsen-Anhalt einen entsprechenden Leitfaden erstellt und veröffentlicht. Zudem unterstützen die medienpädagogischen Berater die Schulen auch in dieser Frage.

Die medienpädagogischen Berater können auch dazu beitragen, datenschutzrechtliche Aspekte der Mediennutzung für den Unterricht beizusteuern. Daneben kommen für diese Aufgabe auch die schulischen Datenschutzbeauftragten in Betracht.

Insoweit bestehen aber weiter gravierende Defizite (vgl. XIII./XIV. Tätigkeitsbericht, Nr. 9.2.1). Zwar hat das Bildungsministerium inzwischen zwei Stellen im Landesschulamt besetzt, die die 788 öffentlichen Schulen insoweit unterstützen sollen. Hilfreich für den Datenschutz in der Schule wirkt auch die Handreichung „Datenschutz an Schulen“ des Bildungsministeriums. Diese Maßnahmen reichen aber in der Praxis keineswegs aus, um die gesetzlichen Anforderungen an die Benennung und das Wirken eines Datenschutzbeauftragten an der Schule als verantwortlicher Stelle zu erfüllen. Der Landesbeauftragte unterstützt das Bildungsministerium bei der Suche nach neuen geeigneten Modellen.

Der Landesbeauftragte wirkte zudem bei der 5. Netzwerktagung des Netzwerkes Medienkompetenz Sachsen-Anhalt (Teil der Landesmedienanstalt) mit und diskutierte u. a. über die Potentiale und Herausforderungen Künstlicher Intelligenz.

Die Sensibilisierung und Aufklärung der Öffentlichkeit über die Risiken der Technik im Zusammenhang mit Datenverarbeitungen, gerade auch für Kinder, bleibt auch durch Art. 57 Abs. 1 lit. b DS-GVO besondere Aufgabe der Datenschutzaufsichtsbehörden. Dies schließt Hinweise zu den Rechten der Betroffenen und zum Selbstdatenschutz ebenso ein wie Informationen zu den einschlägigen Vorschriften und Verarbeitungsgrundsätzen. Es geht also – nicht nur bei Kindern – um Wissens- und Wertevermittlung. Hierfür fehlt dem Landesbeauftragten weiterhin entsprechendes Personal. Ein Personalaufwuchs wird aber auch hier immer dringlicher.

11.2.3 Bildungsmanagementsystem

Im XIII./XIV. Tätigkeitsbericht (Nr. 9.2.3) hatte der Landesbeauftragte das Ziel des Bildungsministeriums beschrieben, ein zentrales landeseinheitliches Softwareprodukt zur Steuerung des Schulbetriebes einzuführen. Das System soll verlässliche operative und statistische Informationen bereitstellen, die Kommunikation zwischen den Akteuren des Schulwesens ebenenübergreifend gewährleisten, automatisierte Datenverarbeitungen ermöglichen (z. B. Schulwechsel) und bei allem die Datenhoheit der Schulen sichern. Hierzu sollte die Neuregelung des § 84f Schulgesetz als Grundlage dienen.

Der Landesbeauftragte wurde vom Bildungsministerium frühzeitig bei der Konzepterstellung einbezogen. Auf die Trennung von Verwaltungsdaten und Statistikdaten wurde seitens des Landesbeauftragten ebenso hingewiesen wie auf die Notwendigkeit eines differenzierten Rollen- und Berechtigungskonzepts. Insgesamt hat der Landesbeauftragte den Aspekt des differenzierten Zugriffs auf die im System zu speichernden Schülerdaten nach Zuständigkeit und Erforderlichkeit betont. Das Bildungsministerium informiert über den Verlauf der Entwicklung u. a. im Rahmen eines Projektbeirates, zu dem neben verschiedenen Landes- und Kommunalbehörden auch der Landesbeauftragte eingeladen wird. Weiter wird der Landesbeauftragte von der Projektleitung des Bildungsministeriums an Beratungsgesprächen beteiligt, um aktuelle datenschutzrechtliche Fragestellungen im laufenden Entwicklungsprozess zu erörtern. Dabei wurden technische und organisatorische Fragen, wie etwa die Verschlüsselung und die Trennung von Datenbeständen, angesprochen und Aspekte

der Verwendung vorhandener Daten für anonyme Auswertungen für bildungspolitische Fragestellungen diskutiert. Der Landesbeauftragte wird das Projekt weiter begleiten.

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.

Weitere Hinweise finden sich im XII. Tätigkeitsbericht (s. Nrn. 5.10, 9.2.2).

11.2.6 Fotografieren in Schulen

Im XV. Tätigkeitsbericht (Nr. 6.3) hatte der Landesbeauftragte Erläuterungen zum Recht am eigenen Bild und zur Verarbeitung von Fotografien von Personen gegeben. Auf den grundsätzlichen Persönlichkeitsschutz und die Rechtsgrundlagen der Verarbeitung, insbesondere unter Berücksichtigung der Wertungen des Kunsturhebergesetzes wurde hingewiesen. Da die Zulässigkeit der Anfertigung und insbesondere Veröffentlichung von Fotoaufnahmen von natürlichen Personen u. a. davon abhängt, wer die Daten verarbeitet, zu welchen Zwecken und in welchen Medien, treten im Einzelfall immer wieder Fragen auf.

Auch im Jahr 2019 stand zum Schuljahresbeginn wieder die Frage der Zulässigkeit von Fotoaufnahmen bei Einschulungsveranstaltungen in der Diskussion. Der Landesbeauftragte hatte hierzu Anfragen zu beantworten. Dabei hat er klargestellt, dass es Schulleitungen aufgrund des Hausrechts gestattet ist, das Fotografieren zu Zwecken des Persönlichkeitsschutzes zu untersagen. Aus datenschutzrechtlicher Sicht ist dies aber nicht zwingend, da es Rechtsgrundlagen und Gestaltungsmöglichkeiten gibt, dem Persönlichkeitsschutz Rechnung zu tragen, ohne den Angehörigen und ggf. anderweitig Interessierten das Fotografieren vollends zu verbieten. Hierzu hat der Landesbeauftragte die „Hinweise zum Fotografieren bei Schulveranstaltungen“ auf seiner Homepage veröffentlicht[13].

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 kla-

[13] https://lsaurl.de/schulvfoto

re 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.

12 Gesundheits- und Sozialwesen

12.1 Gesundheitswesen

12.1.1 Das Digitale-Versorgung-Gesetz

„Die Zukunft der Medizin ist digital“ titelte am 14. November 2019 die Frankfurter Allgemeine Zeitung in ihrem Verlagsspezial. Den Weg dahin soll – im Anschluss an das E-Health-Gesetz von 2016 (vgl. XIII./XIV. Tätigkeitsbericht, Nr. 10.1) – u. a. das Digitale-Versorgung-Gesetz (DVG – Gesetz vom 9. Dezember 2019, BGBl. S. 2562) bereiten. Damit beabsichtigt der Gesetzgeber beispielsweise, digitale Gesundheitsanwendungen zügig in die Versorgung zu bringen, mehr Leistungserbringer an die Telematikinfrastruktur anzuschließen, die Anwendung von Telemedizin zu stärken, Verwaltungsprozesse durch Digitalisierung zu vereinfachen, den Krankenkassen mehr Möglichkeiten zur Förderung digitaler Innovationen zu geben und eine bessere Nutzbarkeit von Gesundheitsdaten für Forschungszwecke zu ermöglichen.

Dabei sorgt insbesondere das Vorhaben, eine zentrale Gesundheitsdatenbank für Forschungszwecke aufzubauen, für Kritik von Datenschützern und Patientenvertretern. In dieser Datenbank sollen pseudonymisiert die Abrechnungsdaten aller gesetzlich Versicherten zu Forschungszwecken gespeichert werden, ohne dass die Betroffenen der Übermittlung ihrer lediglich pseudonymisierten Daten widersprechen können.

Fraglich ist aber auch, ob die Datensicherheit bei sog. Gesundheits-Apps, die künftig in der Regelversorgung verordnet werden können, gewährleistet ist. Zwar ist eine vorherige Prüfung der jeweiligen App auf Datensicherheit, Datenschutz und Funktionalität vorgesehen. Es ist jedoch bekannt, dass Betreiber von Gesundheits-Apps in erheblichem Umfang ohne vorherige Information und Legitimation durch die Nutzer sensible personenbezogene Daten an Tracking-Dienstleister und auch z. B. an Facebook, Google und Amazon weitergeleitet haben sollen (s. auch Nr. 12.1.2).

Das Digitale-Versorgung-Gesetz soll durch ein Patientendatenschutzgesetz ergänzt werden, in dem insbesondere im SGB V Regelungen zu Patientenrechten in der Telematikinfrastruktur getroffen werden. Dies betrifft vornehmlich die elektronische Pa-

tientenakte. Ziel ist aber auch, weitere digitale Anwendungen zu fördern, die Regelungen zur Telematikinfrastruktur und ihrer Anwendungen an technische Weiterentwicklungen und datenschutzrechtliche Vorgaben anzupassen sowie die datenschutzrechtlichen Verantwortlichkeiten festzulegen. Der vorliegende Referentenentwurf zeigt allerdings Erörterungs- und Verbesserungsbedarf auf.

12.1.2 Gesundheitswebseiten und Gesundheits-Apps

Betreiber von Gesundheitswebseiten und Gesundheits-Apps leiten häufig sensible personenbezogene Daten der Nutzerinnen und Nutzer an Dritte weiter. Unter anderem geschieht dies durch Programme, die das Surfverhalten beobachten und analysieren. Von deren Einsatz haben die betroffenen Personen in der Regel keine Kenntnis. Studien ergaben, dass personenbezogene Nutzungsdaten und wohl auch sensible Gesundheitsdaten an verschiedene Interessenten weitergeleitet werden. Die Datenschutzkonferenz forderte die Betreiber von Gesundheitswebseiten und Gesundheits-Apps daher auf, u. a. die Transparenzanforderungen der Datenschutz-Grundverordnung und die Notwendigkeit einer Rechtsgrundlage für die Datenverarbeitung in Gestalt einer ausdrücklichen Einwilligung zu beachten (Entschließung vom 6. November 2019 „Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!“, **Anlage 7**).

12.1.3 IT-Sicherheit im Krankenhaus

Es werden häufiger Vorfälle bekannt, in denen medizinische Einrichtungen von Schadsoftware befallen wurden. Die durch Schadsoftware bewirkte Verschlüsselung von Daten kann in Krankenhäusern zu weitreichenden Beeinträchtigungen des Betriebs führen; dieses Problem verstärkt sich im IT-Verbund einer Trägergesellschaft. Es wurde auch bekannt, dass infolge unzureichender technischer und organisatorischer Vorkehrungen Patientendaten offen im Internet zugänglich waren.

Beim Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist es für einen effektiven Schutz der Patientendaten geboten, nach dem Stand der Technik angemessene Vorkehrungen zu treffen. Dies betrifft alle Einrichtungen unabhängig von ihrer Größe. Die Datenschutzkonferenz hat daher ausdrücklich dazu aufgerufen, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können (Entschließung vom 6. November 2019 „Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten“, **Anlage 8**).

12.1.4 Messengerdienste im Krankenhaus

Messengerdienste haben in den letzten Jahren große Bedeutung für den Austausch von Nachrichten erlangt und zählen im privaten Alltag zu den beliebtesten Kommunikationsformen. Auch im Gesundheitswesen wird in der Praxis gern auf dieses Kommunikationsmedium zurückgegriffen. Gerade im Krankenhaus können verschiedenste Kommunikationsanforderungen damit einfach gewährleistet werden. Da Gesundheitsdaten betroffen sind, ist ein hohes Schutz- und Sicherheitsniveau erforderlich.

Hierzu hat die Datenschutzkonferenz ein Papier ihrer Arbeitsgruppe „Digitalisierung im Gesundheitswesen“ zur Kenntnis genommen, dass die umfänglichen technischen Anforderungen an eine datenschutzkonforme Nutzung von Messengerdiensten formuliert. Das Papier war Gegenstand einer Konsultation mit den einschlägigen Verbänden. Es ist bislang als „Whitepaper“ der DSK auf der Homepage der Datenschutzkonferenz veröffentlicht[14].

12.1.5 Schulärztlicher Gesundheitsdienst

Im XV. Tätigkeitsbericht (Nr. 11.1.4) wurde dargelegt, dass das Landesamt für Verbraucherschutz Sachsen-Anhalt (LAV) plant, die Datenerhebung mittels Elternfragebogen im Rahmen der vorgeschriebenen Schuleingangsuntersuchung auf der Basis von Pflichtangaben durchzuführen (Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 37 Abs. 2 SchulG LSA). Das LAV wird in diesem Zusammenhang als beratend-koordinierende Stelle für den Kinder(zahn)ärztlichen Dienst der Gesundheitsämter Sachsen-Anhalts tätig.

Der Landesbeauftragte hat vorrangig die Erforderlichkeit der Angaben zum familiären Umfeld der Kinder geprüft und anschließend das LAV ausführlich beraten. Bei den fraglichen Daten handelte es sich um Daten zum Sozialstatus des Kindes (Schulbildung und Erwerbstätigkeit der Eltern), zum Migrationshintergrund des Kindes (Geburtsland des Kindes und der Eltern, Nationalität der Eltern), zu Geschwistern des Kindes (Anzahl Geschwister, Anzahl Geschwister im Haushalt, Altersstruktur) und zum Rauchverhalten im Haushalt (Rauchen ja/nein, Rauchen wo). Lediglich hinsichtlich der Angaben zum Migrationshintergrund des Kindes waren die Erläuterungen zur Erforderlichkeit für die Diagnostik im Rahmen der Schuleingangsuntersuchungen überzeugend. Die Erforderlichkeit im Sinne der Unerlässlichkeit der Angaben blieb jedoch im Übrigen trotz der umfänglichen Begründung des LAV zweifelhaft. Im Ergebnis der Beratungen hat das LAV festgelegt, diese Daten weiterhin nur auf freiwilliger Basis mittels Elternfragebogen zu erheben.

Abschließend hat das LAV mit dem Landesbeauftragten nicht nur bei der Schuleingangsuntersuchung, sondern auch bei den übrigen schulärztlichen Untersuchungen und den zahnärztlichen Untersuchungen in der Schule sowie der Kindertagesstätte die Verfahren aus datenschutzrechtlicher Sicht abgestimmt und die entsprechend erforderlichen Unterlagen (Elternfragebögen, Elterninformationsschreiben, Einwilligungserklärungen) überarbeitet.

12.1.6 Krankenhausgesetz

Im Mai 2019 trat die Änderung des Krankenhausgesetzes des Landes in Kraft (GVBl. LSA 2019, S. 76). Ein Schwerpunkt sind die Regelungen zur Verarbeitung von Patientendaten. Mit der Neuregelung liegt nun eine differenzierte, verständliche Befugnisnorm für die Verarbeitung von Patientendaten im Krankenhaus vor. Weiter wird die Verwendung der Daten zu Forschungszwecken nun auf eine klare Grundlage gestellt. Hierzu hatte der Landesbeauftragte die Landesregierung im Vorfeld umfassend beraten. Die Empfehlung des Landesbeauftragten, im Interesse der heutzu-

[14] https://lsaurl.de/messkrank

tage überregionalen Forschung die gesetzlichen Voraussetzungen in den Ländern zu vereinheitlichen, wurde leider nicht aufgegriffen.

Bei den Detailhinweisen des Landesbeauftragten ging es u. a. um den Zugriff auf Daten aus vorheriger Behandlung, die Nutzung von Daten zu Aus- und Fortbildungszwecken, die Voraussetzungen für die Eigenforschung und die Übermittlung für Forschungszwecke. Ausdrücklich zu begrüßen sind die besonderen Schutzvorgaben, die u. a. technische und organisatorische Maßnahmen und die Sensibilisierung der Beschäftigten enthalten. Dank der umfassenden Beratung ist es gelungen, nunmehr im Wesentlichen hinreichend präzise Rechtsgrundlagen zu formulieren, die die Anliegen des Krankenhausbetriebes und die Forschungsinteressen berücksichtigen, aber dennoch einen angemessenen Schutz der Patientendaten und der Patientensouveränität gewähren.

12.1.7 Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke

Die Landesregierung hat einen Gesetzentwurf zur Weiterentwicklung der psychiatrischen Versorgung auf den Weg gebracht (LT-Drs. 7/5251). Im Vorfeld hatte der Landesbeauftragte das zuständige Ministerium für Arbeit, Soziales und Integration zu Einzelfragen beraten. Dabei ging es insbesondere um die Anpassung an die DS-GVO, u. a. im Hinblick auf die Einschränkung von Betroffenenrechten sowie den Einsatz von technischen Mitteln bei Anwendung besonderer Sicherungsmaßnahmen. Im Rahmen der Anhörung durch die Landesregierung wurde ergänzend auf problematische Befugnisse des Psychiatrieausschusses hingewiesen, wonach dieser im Rahmen seiner Besuche auch auf sensible personenbezogene Daten von Patienten mit psychosomatischen Erkrankungen zugreifen kann, ohne dass diese zwangsweise untergebracht sind.

12.1.8 Benennungspflicht von Datenschutzbeauftragten bei Angehörigen von Gesundheitsberufen

Nach Art. 37 Abs. 1 lit. c DS-GVO ist stets ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten nach Art. 9 DS-GVO besteht, wozu u. a. Gesundheitsdaten und genetische Daten gehören. Nach ErwGr 91 Satz 4 soll die Verarbeitung personenbezogener Daten allerdings nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten betrifft und durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufes erfolgt.

Zur Auslegung dieser Vorgaben hat sich die DSK mit ihrer Entschließung vom 26. April 2018 (s. XV. Tätigkeitsbericht, Anlage 1) zur Datenschutzbeauftragten-Bestellpflicht bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs geäußert. Demnach ist bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen, weshalb sie keinen Datenschutzbeauftragten benötigen, auch nicht, wenn sie sich zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen oder ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben.

Etwas anderes gilt nur dann, wenn:

- bei ihren Datenverarbeitungen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten und damit eine Datenschutz-Folgenabschätzung vorgeschrieben ist, z. B. beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen (vgl. Art. 37 Abs. 4 Satz 1 2. Halbsatz DS-GVO i. V. m. § 38 Abs. 1 Satz 2 1. Halbsatz BDSG), oder

- mindestens zehn Personen (einschließlich der Angehörigen der Gesundheitsberufe selbst) in der Regel ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, was sich aus Art. 37 Abs. 4 Satz 1 2. Halbsatz DS-GVO i. V. m. § 38 Abs. 1 Satz 1 BDSG in der ab 25. Mai 2018 anzuwendenden Fassung ableitete.

Mit Wirkung vom 26. November 2019 wurde § 38 Abs. 1 Satz 1 BDSG insoweit geändert, als nunmehr die Grenze, ab der jeder Verantwortliche einen Datenschutzbeauftragten zu benennen hat, bei 20 Personen liegt, die in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Nach Auffassung des Landesbeauftragten führt dies jedoch keineswegs dazu, dass Ärzte, Apotheker oder sonstige Angehörige eines Gesundheitsberufs, die zwar mindestens zehn Personen, aber weniger als 20 Personen in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, künftig keinen Datenschutzbeauftragen mehr benötigen. Vielmehr ist stets im Einzelfall zu prüfen, ob die Kerntätigkeit dieses Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten nach Art. 9 DS-GVO besteht oder wegen des hohen Risikos eine Datenschutz-Folgenabschätzung durchzuführen ist. Dies könnte bei mindestens zehn datenverarbeitenden Personen durchaus häufig der Fall sein.

Auch wenn im Einzelfall die Benennung eines Datenschutzbeauftragten nicht zwingend ist oder ein Grenzfall vorliegt, sollten Verantwortliche aus dem Gesundheitsbereich prüfen, ob sie freiwillig einen Datenschutzbeauftragten benennen (vgl. Art. 37 Abs. 4 Satz 1 1. Halbsatz DS-GVO). Denn unabhängig von der Benennungspflicht müssen sie sicherstellen, dass ausreichend datenschutzrechtlicher Sachverstand vorhanden ist, um der besonderen Sensibilität von Gesundheitsdaten gerecht zu werden (vgl. auch § 22 Abs. 2 Satz 2 Nr. 4 BDSG).

12.1.9 Datenübermittlungen und Werbung nach Verkauf einer Versandapotheke

Den Landesbeauftragten erreichten mehrere Eingaben und Beschwerden zu Datenverarbeitungen, die im Zusammenhang mit dem Verkauf einer Versandapotheke durch einen Apotheker in Sachsen-Anhalt standen.

Datenschutzrechtlich problematisch waren zum einen die Übermittlungen von Kundendaten an den Käufer. Zwar hatte der Verkäufer richtigerweise vorgesehen, dass Datenübermittlungen nur auf der Grundlage einer Einwilligung der jeweils betroffenen Kunden stattfinden, jedoch entsprach die vorformulierte Online-Einwilligungserklärung nicht den Anforderungen der DS-GVO. Sie war nicht gemäß ErwGr 42 in leicht zugänglicher Form und unmissverständlich bereitgestellt.

Die Überschrift und der Haupttext enthielten keinen Hinweis darauf, dass es sich überhaupt um eine datenschutzrechtliche Einwilligungserklärung handeln könnte, sondern stellten Service, Leistungen und Vorteile in den Vordergrund, die mit einer Datenübernahme auf die Datenbank des Erwerbers verbunden wären. Der Text der Einwilligungserklärung war in einer Fußnote unterhalb des Haupttextes sehr kleingedruckt und damit nicht ohne weiteres insbesondere für ältere oder gesundheitlich eingeschränkte Personen lesbar. Der Umstand, dass in die Datenübermittlung auch Gesundheitsdaten einbezogen waren, kam in dem Einwilligungstext nicht deutlich zum Ausdruck. Es entstand der Eindruck, dass die datenschutzrechtliche Einwilligung im „Kleingedruckten“ versteckt werden sollte.

Form und Gestaltung der Einwilligungserklärung verletzten damit die Anforderungen der DS-GVO. Denn eine Einwilligung muss freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben sein (Art. 4 Nr. 11 DS-GVO), im Falle der Verarbeitung von Gesundheitsdaten muss sie sich auch ausdrücklich darauf beziehen (Art. 9 Abs. 2 lit. a DS-GVO). Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Dies gilt auch für eine vom Verantwortlichen vorformulierte Einwilligungserklärung; sie sollte zudem keine missbräuchlichen Klauseln beinhalten. Die betroffene Person muss wissen, dass und in welchem Umfang sie ihre Einwilligung erteilt (Art. 7 Abs. 2 Satz 1 DS-GVO, ErwGr 42).

In diesem Sinne muss:

- die Überschrift klar und deutlich zum Ausdruck bringen, dass es sich um eine datenschutzrechtliche Einwilligung handelt,

- die Erklärung selbst eindeutig als Einwilligungserklärung formuliert sein (z. B. „Ich bin damit einverstanden, dass…“),

- die Erklärung neben dem weiteren Text besonders hervorgehoben und von anderen Inhalten deutlich getrennt sowie in aller Regel vor der Unterschrift platziert werden.

Da der verantwortliche Apotheker die Datenübermittlungen nicht bereits aufgrund der Beratung des Landesbeauftragten einstellte, erging eine Anweisung nach Art. 58 Abs. 2 lit. f DS-GVO (vorübergehende Beschränkung der Datenverarbeitung), mit der die Datenübermittlungen untersagt wurden, solange die vorformulierte Einwilligungserklärung nicht den Anforderungen der DS-GVO entspricht. Die Datenübermittlungen wurden sodann gänzlich eingestellt.

Darüber hinaus war datenschutzrechtlich problematisch, dass der Verkäufer nach dem Verkauf begann, Werbe-E-Mails an seinen alten Kundenstamm zu versenden, mit denen er Produkte aus dem Sortiment der verkauften Versandapotheke anpries und die Kunden unter Verwendung ihrer Bestellhistorie personalisiert ansprach. Der Landesbeauftragte erörterte gegenüber dem Verkäufer, dass für die Verwendung von Gesundheitsdaten aus der Bestellhistorie zu Werbezwecken im Art. 9 Abs. 2 DS-GVO keine Rechtsgrundlage zu finden ist. Der Kontaktaufnahme mittels elektronischer Post zum Zwecke der Werbung für fremde Waren steht zudem § 7 Abs. 2

Nr. 3, Abs. 3 Nr. 2 UWG entgegen, weshalb die Interessenabwägung des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ebenfalls zugunsten der Betroffenen ausfällt. Für diese Werbe-E-Mails bedurfte es somit einer wirksamen und ausdrücklichen Einwilligung der Betroffenen, die nicht vorlag. Der verantwortliche Apotheker stellte daraufhin den Versand der Werbe-E-Mails ein.

12.2 Sozialwesen

12.2.1 Datenpannen

Knapp ein Fünftel der beim Landesbeauftragten eingegangenen Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO betraf Fälle aus dem Bereich des Sozialwesens.

Einen Schwerpunkt bildete dabei das Fehlversenden von Briefen. So wurden Bescheide versehentlich fehlerhaft adressiert. Dadurch wurde unbeteiligten Dritten der Sozialleistungsbezug unbefugt offenbart. Andere Briefe gingen auf dem Postweg verloren. Hier ist der Verbleib der sensiblen personenbezogenen Daten nicht feststellbar. Auch wenn es sich jeweils um Einzelfälle handelt, hat doch jeder Betroffene einen Anspruch darauf, dass das Sozialgeheimnis gewahrt bleibt. Deshalb sollte der verantwortliche Sozialleistungsträger bei jeder Datenschutzverletzung – selbst wenn es sich um einen Einzelfall handelt – prüfen, ob wirklich alles Erforderliche getan wird, um ähnliche Vorfälle künftig zu vermeiden.

Ein weiterer Schwerpunkt betraf Diebstähle aus Kindertagesstätten. In mehreren Fällen wurden Kameras mit Speicherkarte oder Laptops entwendet. Als Maßnahmen zur Verhinderung bzw. weitgehender Vermeidung künftiger Datenschutzverletzungen ähnlicher Art empfiehlt der Landesbeauftragte, Speicherträger in angemessenem Umfang sicher zu verwahren und Daten auf dem PC und mobilen Datenträgern verschlüsselt zu speichern. Der Zugang zum laufenden PC sollte durch Passwort gesichert sein und nach mehrmaliger Falscheingabe sollte eine Sperrung eintreten. In Bezug auf Kameras sind eine tägliche Datensicherung von der Speicherkarte vorzunehmen und die Daten darauf zu löschen.

12.2.2 Umgang mit Nachweisen bei selbständig Tätigen

Selbständig Tätige erhalten zusätzliche Leistungen nach dem SGB II, wenn diese ihren Lebensunterhalt mit den Einnahmen aus ihrer selbständigen Tätigkeit nicht ausreichend sicherstellen können. Anhand der Angaben im Antrag und der Nachweise prüfen die zuständigen Behörden – die Jobcenter – den Leistungsanspruch. Nach Einführung der DS-GVO haben viele selbständig tätige Antragsteller das Einreichen von Nachweisen, aus denen Daten ihrer Kunden, Geschäftspartner, Mitarbeiter oder Lieferanten hervorgehen, mit der Begründung verweigert, nicht zur Übermittlung dieser Daten an das Jobcenter berechtigt zu sein. Darüber hinaus stellte sich die Frage, ob sie verpflichtet sein könnten, diesen betroffenen Personen mitzuteilen, dass sie die Daten an das Jobcenter weitergeleitet haben.

Zur Wahrung des Sozialdatenschutzes ist grundsätzlich zu beachten, dass Jobcenter nur die Daten erheben dürfen, die für die Erfüllung der Aufgaben, hier für die Prüfung, ob ein Leistungsanspruch besteht, erforderlich sind. Es dürfte nicht immer für die Prüfung des Leistungsanspruchs erforderlich sein, auch Daten von Kunden, Ge-

schäftspartnern, Mitarbeitern und Lieferanten zu erheben. Sofern es jedoch im Einzelfall unumgänglich ist, solche Daten zu nennen, ist Art. 6 Abs. 1 lit. f DS-GVO Grundlage für die Offenbarung durch den Antragsteller gegenüber dem Jobcenter. Danach ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Antragstellers erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Dritten überwiegen. Die berechtigten Interessen des Antragstellers auf Sozialleistungen liegen in der Wahrnehmung seines grundrechtlich geschützten Anspruchs auf Wahrung eines menschenwürdigen Existenzminimums. Hierfür muss das Jobcenter in die Lage versetzt werden, anhand der vorgelegten Unterlagen seinen Anspruch zu prüfen und festzustellen. Im Rahmen der gebotenen Interessenabwägung ist zu berücksichtigen, dass die in den Unterlagen enthaltenen Daten, die dem Jobcenter im Rahmen der Antragstellung bekannt werden, dem Sozialgeheimnis unterliegen. Infolge dieses Schutzes können die Interessen des Antragstellers überwiegen.

Besteht dann aber auch die Verpflichtung, den betroffenen Personen die Weiterleitung ihrer Daten an das Jobcenter mitzuteilen? Zwar könnte grundsätzlich eine Informationspflicht nach Art. 13 Abs. 1 lit. e DS-GVO bestehen. Zu beachten ist jedoch, dass gem. Art. 23 DS-GVO diese Pflicht u. a. zum Schutz der Rechte und Freiheiten anderer Personen, zu denen auch der selbständig Tätige als datenschutzrechtlich Verantwortlicher zählt, beschränkt werden kann (Art. 23 Abs. 1 lit. i DS-GVO). Diese Beschränkung findet sich im nationalen Recht in § 32 BDSG. Nach § 32 Abs. 1 Nr. 4 BDSG besteht die Verpflichtung zur Information der betroffenen Person nicht, wenn die Erteilung der Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen. Die selbständig Tätigen könnten gehindert sein, ihren grundrechtlich geschützten Anspruch auf Wahrung eines menschenwürdigen Existenzminimums geltend zu machen, wenn sie dadurch ihren Sozialleistungsbezug gegenüber ihren Kunden, Geschäftspartnern, Lieferanten und Mitarbeitern offenbaren und daraus folgend negative Auswirkungen auf ihre selbständige Tätigkeit befürchten müssten. Deshalb dürfte hier die erforderliche Interessenabwägung grundsätzlich zugunsten der selbständig Tätigen ausfallen, so dass eine Informationsverpflichtung zu verneinen ist.

13 Statistik, Kommunales

13.1 Zensus 2021

13.1.1 Zensusvorbereitungsgesetz 2021

Im Januar 2019 ist eine Änderung des Zensusvorbereitungsgesetzes 2021 des Bundes in Kraft getreten (vgl. XV. Tätigkeitsbericht, Nr. 12). Mit Einführung eines neuen § 9a sollten die Übermittlungswege und die Qualität der zum Zensus 2021 zu übermittelnden Daten aus den Melderegistern geprüft und die Programme für die Durchführung des Zensus 2021 getestet und weiterentwickelt werden. Mittel zum Zweck war die Übermittlung von bis zu 46 teils hoch sensiblen differenzierbaren Merkmalen aller über 82 Millionen in der Bundesrepublik gemeldeten Personen durch die Meldebehörden an die Statistischen Ämter.

Der gegen diesen Volltest mit Echtdaten beim Bundesverfassungsgericht gestellte Antrag auf Erlass einer einstweiligen Anordnung wurde mit Entscheidung vom 6. Februar 2019 abgelehnt (Az.: 1 BvQ 4/19, juris).

Daraufhin hat der initiierende Verein gemeinsam mit dem Arbeitskreis Zensus Verfassungsbeschwerde gegen die massenhafte Übermittlung von Meldedaten im Rahmen eines Testlaufes für den Zensus 2021 eingelegt, wie seiner Internetpräsenz[15] zu entnehmen ist. Eine Entscheidung des Bundesverfassungsgerichtes bleibt abzuwarten.

13.1.2 Zensusgesetz 2021

Der Zensus 2021 rückt nun näher (vgl. XV. Tätigkeitsbericht, Nr. 12). Er ist, wie schon der Zensus 2011, als registergestützte Erhebung konzipiert. Der Zensus 2021 umfasst eine Bevölkerungszählung, eine Gebäude- und Wohnungszählung als Vollerhebung, eine Haushaltebefragung auf Stichprobenbasis und Erhebungen an Anschriften mit Sonderbereichen. Dabei werden in erster Linie bereits vorhandene Verwaltungsdaten genutzt und – so heißt es in der Gesetzesbegründung – nur dann ergänzende Erhebungen durchgeführt, wenn Verwaltungsdaten für bestimmte Merkmale nicht vorhanden oder aus statistischer Sicht nicht für die Auswertung geeignet sind. Neben Übermittlungen behördlicher Daten, insbesondere Melderegisterdaten und Daten der Bundesagentur für Arbeit, sind also auch wieder ergänzende primärstatistische Befragungen der Bevölkerung vorgesehen.

Bereits Ende des Jahres 2018 hatte der Landesbeauftragte Gelegenheit, im Rahmen einer Sitzung der Ad-hoc-Arbeitsgruppe Zensus 2021 des Arbeitskreises Statistik der DSK mit dem Bundesministerium des Innern, für Bau und Heimat einen Referentenentwurf eines Gesetzes zur Durchführung des Zensus im Jahr 2021 (Zensusgesetz 2021 – ZensG 2021) zu beraten.

Das ZensG 2021 (BT-Drs. 19/8693) ist vom Bundestag am 6. Juni 2019 beschlossen worden. Allerdings hielt der Bundesrat das Gesetz für veränderungs- und ergänzungsbedürftig, sodass der Vermittlungsausschuss angerufen wurde.

Die Beschlussempfehlung des Vermittlungsausschusses, die am 7. November 2019 vom Bundestag (BT-Drs. 19/14700) und am 8. November 2019 vom Bundesrat (BR-Drs. 595/19 (Beschluss)) angenommen wurde, enthält jedoch eine datenschutzrechtlich problematische Ergänzung.

Nach dem neuen § 34 ZensG 2021 wird das Statistische Bundesamt verpflichtet, „…auf Anfrage eines Statistischen Landesamtes für dessen Zuständigkeitsbereich eine Kopie der Zensusdaten aus der Auswertungsdatenbank sowie eine Kopie der Daten zu den Merkmalen nach § 4 Nr. 4 bis 6 ZensVorbG 2021 aus den zentral im Statistischen Bundesamt gespeicherten Daten für ausschließlich statistische Zwecke des Landes im Rahmen des § 1 Abs. 3 Nr. 3 zu übermitteln.“ Eine vergleichbare Vorschrift zur Datenbereitstellung gegenüber den Statistischen Ämtern der Länder war im ZensG 2011 nicht enthalten.

[15] https://lsaurl.de/zen2021

Was nach folgerichtiger Teilhabe der Länder an dem im Bundesamt vorhandenen Datenschatz ausschaut, hat gleich mehrere Haken:

Zunächst fehlt es der Formulierung an einer normenklaren Löschfrist für die in die Statistischen Landesämter übermittelten Daten. Der Verweis auf die in § 16 Abs. 1 ZensVorbG 2021 genannte Löschfrist ist nicht optimal. Davon abgesehen, dass durch den Querverweis das ZensG 2021 selbst schwerer lesbar wird, ist die Verweisnorm auch nicht wirklich erhellend. Zwar ist dort eine grundsätzliche Löschfrist von 6 Jahren nach dem Zensusstichtag angegeben, was aber durch einen Weiterverweis von dort auf § 15 ZensVorbG 2021 für die Angaben aus dem Steuerungsregister nicht gilt. Eine Speicherung von unbestimmter Dauer wäre damit nicht auszuschließen.

Darüber hinaus sind in dem damit freigegebenen Datenbestand auch Teile des Zensustestlaufes nach dem ZensVorbG 2021 enthalten, gegen das eine Verfassungsbeschwerde eingelegt worden ist (vgl. Nr. 13.1.1).

Das ZensG 2021 ist am 2. Dezember 2019 verkündet worden (BGBl. I S. 1851) und am 3. Dezember 2019 in Kraft getreten.

Der Landesbeauftragte führte mit dem Ministerium für Inneres und Sport und dem Statistischen Landesamt eine umfangreiche Beratung zu Inhalten eines Landesausführungsgesetzes zum Zensus 2021 sowie zur Vorbereitung und praktischen Durchführung des Zensus durch. Der Gesetzentwurf regelt insbesondere die Einrichtung und Organisation der Erhebungsstellen in den Kommunen.

13.1.3 Ausführungsgesetz des Landes Sachsen-Anhalt zum Zensusgesetz 2021

Mit dem am 3. Dezember 2019 in Kraft getretenen Zensusgesetz 2021 wurde die Durchführung des Zensus 2021 als Volks-, Gebäude- und Wohnungszählung im Jahr 2021 angeordnet (vgl. Nr. 13.1.2). Durch das Gesetz wurde jedoch nur der Rechtsrahmen für die Erhebungen geschaffen. Der Erlass von Vorschriften über die Einrichtung von Erhebungsstellen und zur Organisation der einzelnen Erhebungen blieb den Landesgesetzgebern überlassen.

Dem soll der Gesetzentwurf eines Ausführungsgesetzes des Landes Sachsen-Anhalt zum Zensusgesetz 2021 (E-ZensAG 2021 LSA) Rechnung tragen. Er soll die ergänzenden Vorschriften zur Zensusdurchführung enthalten.

Der Landesbeauftragte äußerte sich gegenüber dem Ministerium für Inneres und Sport als federführendem Fachministerium mit einer Reihe von Hinweisen und Anmerkungen.

Die Gebäude- und Wohnungszählung als Vollerhebung nimmt das Landesamt für Statistik wahr. Dieses kann sich zur Aufgabenerfüllung Dritter bedienen. Soweit die Auskünfte von den Auskunftspflichtigen nicht online erteilt werden, würde unter Umständen die gesamte Prozesskette zwischen dem Versand der Erhebungsunterlagen und der Entgegennahme der fertig digitalisierten Einzelangaben von Auftragnehmern erledigt werden können. Der Landesbeauftragte hat dazu die Frage gestellt, ob die Gesetzesformulierung zu einer Auftragsvergabe für „einzelne Tätigkeiten“ noch die Gebote der Normenbestimmtheit und der Transparenz gegenüber den Bürgerinnen

und Bürgern erfüllt. Besonders problematisch ist die Absicht, die Erhebung auch durch Telefoninterviews vorzusehen und diese Tätigkeit ebenfalls einem Dienstleister zu übertragen. Dies würde bedeuten, dass neben das Landesamt für Statistik ein Privater als Erhebungsstelle tritt.

In dem von der Landesregierung in den Landtag eingebrachten Gesetzentwurf (LT-Drs. 7/5732) sind diese Einwände zugunsten einer normenklaren Regelung weitgehend aufgegriffen worden.

Die örtliche Durchführung des Zensus 2021 soll den Gemeinden übertragen werden. Dies betrifft insbesondere die Stichprobenerhebung in Haushalten. Bedenken des Landesbeauftragten gegen die mögliche Verhängung von Bußgeldern wegen Verstößen gegen Mitwirkungspflichten von Bürgern als Erhebungsbeauftragte wurden dagegen im Gesetzentwurf nicht berücksichtigt.

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 personen-

bezogenen 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.

14 Wirtschaft

14.1 Erforderliche Datenschutzkompetenzen bei kleinen und mittleren Unternehmen

Auch im aktuellen Berichtszeitraum gingen zahlreiche Informations- und Beratungsanfragen von kleinen und mittleren Unternehmen (KMU) ein. Leider richteten sich ebenfalls viele Beschwerden gegen diese Unternehmen (s. auch Nr. 2.1).

KMU verarbeiten mitunter eine Fülle von unterschiedlichen personenbezogenen Daten. Dazu gehören:

- Kontakt- und Vertragsdaten von Geschäftspartnern in Papierform und auf Personalcomputern oder mobilen Datenträgern, z. B. Handys;
- Daten, die auf der Homepage erhoben werden, z. B. durch Online-Formulare und Trackingprogramme;
- eine Vielzahl von Daten, die in branchenspezifische Verwaltungsprogramme gespeichert werden, z. B. Auftragsabwicklung für Handwerker; diese Programme werden häufig auch für Datenübermittlungen, z. B. im Falle von Gesundheitsunternehmen auch für die Übermittlung von Gesundheitsdaten, genutzt;
- häufig werden Firmenclouds genutzt, in denen Daten von Geschäftspartnern gespeichert werden, damit diese auch online abrufbar sind;
- in vielen Geschäften mit offenen Warenauslagen wird auch während der Öffnungszeiten eine Videoüberwachung durchgeführt, unter Umständen mit der Möglichkeit des Fernzugriffs;
- die Personalverwaltung erfolgt entweder durch Personalakten in Papierform oder zumindest teilweise elektronisch; mitunter erfolgen elektronische Übermittlungen, z. B. an Steuerberater zur Durchführung der Lohnbuchhaltung.

Aus diesen Verarbeitungen ergeben sich unter anderem folgende Fragestellungen: Sind die Verarbeitungen auf das erforderliche Maß beschränkt? Sind Informationspflichten gegenüber Kunden und Besuchern der Homepage erfüllt? Sind die Doku-

mentationspflichten umgesetzt, wird das Verzeichnis der Verarbeitungstätigkeiten geführt? Verfügt der Rechner über aktuelle Software, Virenschutz und Firewall, sodass die darauf gespeicherten Daten verfügbar sind und Angriffe abgewehrt werden können? Ist bei Nutzung eines Dienstleisters (z. B. Clouddienst) ein datenschutzgerechter Vertrag über eine Auftragsverarbeitung abgeschlossen? Sind Datenübermittlungen im erforderlichen Umfang verschlüsselt? Ist die Videoüberwachung auf das für den Zweck erforderliche Maß beschränkt?

KMU sind – genauso wie Großunternehmen – verantwortlich für durch sie vorgenommene Verarbeitungen personenbezogener Daten, Art. 4 Nr. 7 DS-GVO. Um dieser Verantwortung gerecht zu werden und die Vorschriften des Datenschutzes einzuhalten, bedarf es vor allem rechtlicher und technischer Kompetenzen. Berufsausbildungen oder auch z. B. Lehrgänge zur Vorbereitung auf Meisterprüfungen reichen hier nicht aus, die Kompetenzen zu vermitteln.

Es müssen durch KMU also zusätzliche Kompetenzen erworben werden. Dies kann durch Schulungen der Mitarbeiter, durch einzuholende Informationen z. B. von Kammern und Branchenverbänden oder insbesondere durch die Tätigkeit des betrieblichen Datenschutzbeauftragten erfolgen.

Bislang war die Benennung von Datenschutzbeauftragten erforderlich, soweit das Unternehmen mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt hat. Die Bezugszahl hat sich nunmehr von zehn auf 20 Personen erhöht, § 38 Abs. 1 Satz 1 BDSG (s. Nr. 4.1.1). Gleichwohl gelten nach wie vor weitere Regelungen, nach denen ein Datenschutzbeauftragter zu benennen ist. So ist nach § 38 Abs. 1 Satz 2 BDSG ein Datenschutzbeauftragter zu benennen, wenn eine Datenschutz-Folgenabschätzung durchzuführen ist oder personenbezogene Daten zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung verarbeitet werden. Nach Art. 37 Abs. 1 DS-GVO ist im nichtöffentlichen Bereich ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit in der Durchführung von Verarbeitungen, welche eine umfangreiche regelmäßige und systematische Überwachung erforderlich machen, oder in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Der Landesbeauftragte betont in seinen Beratungen folgende zusätzliche Empfehlung: Unternehmen, die nach dieser Rechtslage keinen Datenschutzbeauftragten benennen müssen, sollten prüfen, ob die Art und Weise sowie der Umfang der verarbeiteten personenbezogenen Daten und die sich daraus ergebenden Risiken für die betroffenen Personen eine fakultative Benennung eines Datenschutzbeauftragten nach Art. 37 Abs. 4 DS-GVO erfordern.

14.2 Meldungen von Datenschutzverletzungen

Die Meldungen von Datenschutzverletzungen gem. Art. 33 DS-GVO haben im Berichtszeitraum deutlich zugenommen (vgl. XV. Tätigkeitsbericht, Nr. 13.3). Allein aus dem Bereich der Wirtschaft (ohne Unternehmen aus dem Sozial- und Gesundheitsbereich) gingen 115 Meldungen ein. Gegenstände der Meldungen, die Hinweise des Landesbeauftragten zu Abhilfemaßnahmen der Verantwortlichen auslösten, betrafen insbesondere:

- Versendungen von Briefpost an Nichtberechtigte

  Häufig erfolgten fehlerhafte Adressierungen, z. B. bei Gleichheit des Nachnamens. Erhebliche Risiken für betroffene Personen bestehen z. B. dann, wenn Kontodaten oder Beschäftigtendaten einen nicht beabsichtigten Empfänger erreichen und dieser den Brief öffnet. Der Landesbeauftragte empfahl genau zu prüfen, ob der im Adressfeld angegebene Empfänger auch der beabsichtigte ist. Hier kann das Vier-Augen-Prinzip oder eine deutliche Sensibilisierung der Beschäftigten, die mit der Versendung betraut sind, helfen. Soweit Unberechtigte die Briefpost erhalten haben, sollten sie gebeten werden, diese an den Absender zurückzugeben. Zudem sollten sie darauf hingewiesen werden, dass sie keine Berechtigung haben, diese Daten aus der Briefpost zu verarbeiten.

- Versendung von E-Mails an nicht beabsichtigten Empfänger sowie mit offenem Verteiler

  Mehrfach gelangten auch E-Mails an Empfänger, die diese E-Mails nicht erhalten sollten. Das geschah z. B. durch die fehlerhafte Eingabe einer E-Mailadresse oder durch die Nutzung eines falschen E-Mailverteilers. Erhebliche Risiken für die betroffenen Personen können hier insbesondere dann entstehen, wenn in der E-Mail besonders geheimhaltungswürdige Daten (z. B. besondere Kategorien personenbezogener Daten oder Bank- oder andere detaillierte Vermögensdaten) übermittelt werden. Schutz bietet hier große Sorgfalt bei der Eingabe der E-Mail-Adresse bzw. des Verteilers oder die E-Mail-Verschlüsselung.

  Seit mehreren Jahren gehen beim Landesbeauftragten regelmäßig Meldungen mit dem Inhalt ein, dass E-Mails mit offenem Verteiler versandt wurden. Hier hilft die sorgfältige Auswahl des Versendungsmodus Blindkopie bzw. BCC oder eine entsprechende Voreinstellung im E-Mail-Programm, wodurch die jeweiligen Empfänger anderen Empfängern nicht mitgeteilt werden.

- Versendung von E-Mails durch den Virus „Emotet“

  Dieser Virus nutzt die Adressbücher von E-Mail-Programmen und versendet ohne Zutun des Berechtigten E-Mails. Der Landesbeauftragte wies in den gemeldeten Fällen auf die Homepage des BSI hin. Dort werden geeignete Schutzmaßnahmen beschrieben und Verhaltenshinweise gegeben.[16]

- Abhandengekommene Datenträger

  Auch in diesem Berichtszeitraum sind wieder Datenträger abhandengekommen, auf denen sich mitunter sensible personenbezogene Daten befanden. So wurden ganze Personalcomputer aus Räumen entwendet oder mobile Datenträger auf Reisen verloren. In mehreren Fällen nahmen Familienangehörige bzw. enge „Freunde“ dienstlich genutzte Datenträger an sich, um den Besitzer zu kompromittieren. Der Landesbeauftragte wies bereits in Nr. 13.3 sei-

[16] https://lsaurl.de/emobsi

nes XV. Tätigkeitsberichts auf notwendige Verschlüsselungen hin. Sofern Datenträger mit einer aktuellen Software und einem sicheren Passwort verschlüsselt werden, ist eine Kenntnisnahme der darauf gespeicherten personenbezogenen Daten nahezu ausgeschlossen.

- Entsorgung von Unterlagen mit personenbezogenen Daten im Papiermüll

  In einem Fall wurden Unterlagen, die detaillierte Informationen über das Vermögen zahlreicher betroffener Personen enthielten, im Papiermüll entsorgt. Der Landesbeauftragte wies darauf hin, dass Datenträger in Papierform – aber auch elektronische Datenträger – so entsorgt werden müssen, dass Unberechtigte keine Kenntnis der darauf gespeicherten personenbezogenen Daten erlangen können. Dies gelingt unter Berücksichtigung der Norm DIN 66399 „Büro- und Datentechnik – Vernichten von Datenträgern“. Im Falle der Entsorgung von Papiermüll sollten insbesondere Reinigungskräfte – auch solche, die nur vertretungsweise tätig werden – im Rahmen der datenschutzrechtlichen Belehrung genau darüber informiert werden, wie der Papiermüll zu entsorgen ist.

- Kompromittierung eines Amazon-Kontos

  Ein Unternehmen berichtete, dass sein Konto bei Amazon durch einen Unbekannten übernommen wurde, welcher fiktive Artikel zu unterdurchschnittlichen Preisen anbot, um sich am Erlös zu bereichern. Richtigerweise hat der Unternehmer sein Amazon-Konto sofort sperren lassen. Da nicht ausgeschlossen werden konnte, dass der Angreifer das Amazon-Konto mit Hilfe der E-Mail-Adresse, welche für dieses Konto genutzt wird, übernommen hat, riet der Landesbeauftragte, ein neues Passwort für diese E-Mail-Adresse einzugeben. Schutz vor derartigen Angriffen bietet vor allem die von Amazon angebotene 2-Faktor-Authentifizierung.

- Verschlüsselung durch Schadsoftware

  In einigen Fällen wurde die Verschlüsselung von Dateien durch Schadsoftware gemeldet. Damit waren personenbezogene Daten für den Verantwortlichen entgegen Art. 32 Abs. 1 lit. b DS-GVO nicht verfügbar. Auch hier verwies der Landesbeauftragte auf die Empfehlungen des BSI.[17]

- Fehlerhafte Zuordnung von Unterlagen

  Durch die Aufnahme von Unterlagen in falsche Akten ist ebenfalls die Verfügbarkeit der personenbezogenen Daten nicht gewährleistet. In einem gemeldeten Fall wurden die fehlerhaft zugeordneten Unterlagen allerdings nach langer Suche aufgefunden und richtig zugeordnet.

- Doppelte Vergabe von Sendungsnummern

  Ein Unternehmen meldete, dass in etlichen Fällen Sendungsnummern für Pakete, die nur einem Kunden zugeordnet werden sollten, doppelt vergeben

[17] https://lsaurl.de/ransombsi

wurden. Mit dieser Sendungsnummer soll der berechtigte Empfänger erfahren können, wo sich seine Bestellung befindet und wann er sie dort abholen kann. Die doppelte Vergabe der Sendungsnummer führte dazu, dass jeweils ein zweiter Kunde die Sendung eines nicht an ihn gerichteten Pakets verfolgen konnte.

14.3 Erfüllung der Betroffenenrechte

Viele Anfragen von Unternehmen und Beschwerden von betroffenen Personen hatten die Erfüllung der Betroffenenrechte zum Inhalt. Häufig musste der Landesbeauftragte feststellen, dass die einschlägigen Vorschriften der DS-GVO von Verantwortlichen nicht beachtet oder die Rechte von den betroffenen Personen zu weitgehend eingefordert wurden. Es waren daher in vielen Fällen Hinweise zur Erfüllung dieser Pflichten gegenüber Verantwortlichen und zu den Grenzen der Rechte gegenüber den betroffenen Personen erforderlich.

Die Rechte der betroffenen Personen sind in Art. 12 bis 22 DS-GVO geregelt. Mit Hilfe dieser Rechte sollen betroffene Personen die Verarbeitung ihrer personenbezogenen Daten genauer nachvollziehen und besser über die Verwendung ihrer Daten bestimmen können. Sie sind daher von erheblicher Bedeutung.

Zur Geltendmachung der Betroffenenrechte hat der Landesbeauftragte zusammen mit der Verbraucherzentrale Sachsen-Anhalt e. V. im Berichtszeitraum ein Faltblatt herausgegeben, welches auf der Homepage abrufbar ist und in ausgedruckter Form bestellt werden kann.[18]

In etlichen Fällen baten betroffene Personen den Landesbeauftragten, stellvertretend für sie ihre Rechte gegenüber den Verantwortlichen geltend zu machen. Dies ist jedoch nicht seine Aufgabe. Allerdings hat er die Anwendung der DS-GVO zu überwachen und durchzusetzen. Werden gegenüber dem Verantwortlichen geltend gemachte Betroffenenrechte nicht gänzlich erfüllt, hat der Landesbeauftragte die Befugnis, von den Verantwortlichen z. B. Auskünfte zu verlangen, Datenschutzüberprüfungen durchzuführen oder Verantwortliche und Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Personen auf Ausübung ihrer Rechte zu entsprechen. Von allen diesen Befugnissen machte er mehrfach Gebrauch.

Informationspflichten

Die Informationen nach Art. 13 und 14 DS-GVO müssen der betroffenen Person lediglich mitgeteilt werden. Der dafür nötige Nachweis kann z. B. durch Empfangsbestätigungen, einen Absende- bzw. Aktenvermerk oder durch praktizierte betriebliche Übungen aufgrund von betriebsinternen Verfügungen erbracht werden.

Die betroffene Person muss dieser Informationsmitteilung nicht zustimmen. In einigen Fällen stellte der Landesbeauftragte daher klar, dass Personen durch die Entgegennahme der Informationen nicht ihre Einwilligung in die Datenverarbeitung erteilen. Insoweit ist die Mitteilung dieser Information von den Fällen zu unterscheiden, in denen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten eine Einwilligung nach Art. 7 DS-GVO erforderlich ist. Nur die Einwilligung verlangt eine eindeu-

[18] https://lsaurl.de/IhreDaten

tige bestätigende Handlung, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist.

In zahlreichen Fällen war festzustellen, dass die Informationspflichten auf Homepages unzureichend erfüllt wurden. Hier ist insbesondere darauf zu achten, dass über alle Zwecke der Verarbeitung personenbezogener Daten informiert wird. Dies gilt zumal für personenbezogene Daten, die schon beim Aufrufen der Homepage erhoben werden (z. B. IP-Adresse, Browserinformationen, Sprache, Betriebssystem) und auch für Daten, die durch den Nutzer in Online-Formularen eingetragen werden (z. B. Kontaktdaten, Bestellungen etc.). Auch wurde nicht immer über die Empfänger – einschließlich der Auftragsverarbeiter – oder die Kategorien von Empfängern informiert.

Auskunftsrecht

In vielen Beschwerden wurde beklagt, dass für die Datenverarbeitung Verantwortliche die Pflicht zur Auskunft nach Art. 15 DS-GVO nicht erfüllen würden, insbesondere keinerlei Reaktion des Verantwortlichen auf das Auskunftsersuchen erfolgte. Auch wurden Auskünfte sehr zögerlich und unvollständig erteilt.

Der Landesbeauftragte wies in diesen Fällen auf die notwendigen Inhalte der zu erteilenden Auskunft hin (Art. 15 Abs. 1 und 2 DS-GVO) und darauf, dass die Auskunft unverzüglich, jedenfalls aber innerhalb eines Monats, zu erteilen ist. Eine Verlängerung dieser Frist ist nur möglich, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist (Art. 12 Abs. 3 DS-GVO).

In anderen Fällen stellte der Landesbeauftragte klar, dass die betroffenen Personen ihr Auskunftsrecht zu weitgehend beanspruchten. Der Auskunftsanspruch nach Art. 15 DS-GVO umfasst grundsätzlich nicht das Recht auf Übersendung vollständiger Schriftstücke oder gar Akten. Denn es handelt sich um ein Auskunftsrecht, nicht um ein Akteneinsichtsrecht.

Nach Art. 15 Abs. 3 DS-GVO besteht nur ein Anspruch auf eine Kopie – hiermit ist nicht zwingend eine Fotokopie gemeint – der eigenen personenbezogenen Daten. Das beinhaltet lediglich den Anspruch auf eine verkörperte Auskunft ausschließlich zu den verarbeiteten personenbezogenen Daten des Antragstellers (z. B. Ausdruck), damit er in der Lage ist, seine weiteren Betroffenenrechte geltend zu machen.

Zudem darf eine Auskunft nicht die Rechte anderer Personen beeinträchtigen (Art. 15 Abs. 4 DS-GVO). So hat der Verantwortliche die Daten Dritter vor der Bereitstellung von Fotokopien regelmäßig zu schwärzen.

Recht auf Löschung

Im Zusammenhang mit Beschwerden gegen unterbliebene Löschungen personenbezogener Daten wies der Landesbeauftragte mehrfach darauf hin, dass die Pflicht zur Löschung gem. Art. 17 DS-GVO unabhängig von einem gestellten Löschungsantrag besteht, insbesondere dann, wenn der Zweck, für welchen die Daten erhoben worden sind, nicht mehr existiert bzw. die Verarbeitung der Daten für diesen Zweck nicht mehr erforderlich ist.

In manchen Fällen kann der für die Datenverarbeitung Verantwortliche Grund zu der Annahme haben, dass die Datenlöschung schutzwürdige Interessen der betroffenen Person beeinträchtigen könnte. Er darf dann die jeweiligen Daten weiter ausschließlich zu dem Zweck speichern, die betroffene Person – soweit für ihn möglich und zumutbar – zu informieren (§ 35 Abs. 2 BDSG). Sie soll dann selbst über eine Löschung entscheiden können, was ihr der für die Datenverarbeitung Verantwortliche – hier durch sachgerechte Information – erleichtern muss (Art. 12 Abs. 2 Satz 1 DS-GVO).

14.4 Wohnungswirtschaft

14.4.1 Daten zu Vergleichswohnungen zur Begründung von Mieterhöhungsverlangen

An den Landesbeauftragten trugen Vermieter verschiedene Anfragen heran. Dazu gehörte die Frage, unter welchen Bedingungen Informationen über Vergleichswohnungen, die zur Begründung eines Mieterhöhungsverlangens nach § 558a Abs. 2 Nr. 4 BGB geeignet sind, verarbeitet werden dürfen.

Konkrete Informationen über Vergleichswohnungen, wie sie nach der Rechtsprechung des Bundesgerichtshofes zur gerichtsfesten Begründung eines Mieterhöhungsverlangens erforderlich sind (BGH vom 18. Dezember 2002, Az. VIII ZR 141/02, z. B. Adresse, Größe, Ausstattung, Miethöhe, Beschreibung der genauen Lage der Wohnung im Geschoss oder Bezeichnung einer nach außen erkennbaren Wohnungsnummer), sind auch ohne Namensnennung des Mieters der Vergleichswohnung personenbeziehbar im Sinne von Art. 4 Nr. 1 DS-GVO. Nach Auffassung des Landesbeauftragten kommt als gesetzliche Rechtsgrundlage für das Nutzen von Informationen aus dem eigenen Mietbestand oder auch das Einholen dieser Informationen bei einem anderen Vermieter und das Benennen dieser Daten im Mieterhöhungsverlangen die Interessenabwägungsklausel des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Aus § 558a Abs. 2 Nr. 4 BGB lässt sich ein diesbezügliches von der Rechtsordnung anerkanntes berechtigtes Interesse des Vermieters und auch des Adressaten des Mieterhöhungsverlangens ableiten. Letzterer muss die Berechtigung des Verlangens nachprüfen können, indem er die genannte Vergleichswohnung ohne nennenswerte Schwierigkeiten auffinden, sich über die Vergleichswohnung informieren und die behauptete Vergleichbarkeit nachvollziehen kann (BGH, a. a. O.).

Zu beachten ist, dass im Sinne des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) im Mieterhöhungsverlangen auf das Nennen des Namens des betroffenen Mieters verzichtet werden sollte, wenn die Vergleichswohnung mit Adresse, Geschoss, ggf. Ausrichtung (links/rechts/Mitte) und ggf. Wohnungsnummer hinreichend genau beschrieben werden kann. Voraussetzung ist zudem, dass der Vermieter den betroffenen Mieter zuvor rechtzeitig auf die beabsichtigte Datenübermittlung und das sich daraus für ihn ergebende Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO hingewiesen hat (Art. 21 Abs. 4 DS-GVO). Dabei ist auch ein allgemeiner Hinweis auf das Widerspruchsrecht, z. B. zu Beginn des Mietverhältnisses, im Hinblick auf künftig auftretende derartige Datenübermittlungen denkbar. Dieser Hinweis müsste wegen Art. 21 Abs. 4 2. Halbsatz DS-GVO allerdings von den Informationen nach Art. 13, 14 DS-GVO getrennt erfolgen.

14.4.2 Übermittlung von Mieterdaten an Träger der Wohnungslosenhilfe

Vermieter erkundigten sich, ob sie Daten von Mietern und aus Mietverhältnissen an (so genannte) Träger der Wohnungslosenhilfe übermitteln dürfen. Die Übermittlung sollte dem Ziel dienen, Mietern Beratung und Hilfe durch diese Stellen zukommen zu lassen, um das Mietverhältnis zu stabilisieren.

Eine gesetzliche Rechtsgrundlage, die pauschal eine Datenübermittlung von Vermietern an gesetzliche Sozialleistungsträger oder auch an freie Träger erlaubt, die Wohnungslosen und von Wohnungslosigkeit bedrohten Personen Beratungs- und Unterstützungsleistungen anbieten, ist nicht ersichtlich. Denn die Übermittlungen sind nach Auffassung des Landesbeauftragten nicht zur Erfüllung des Mietvertrages erforderlich (Art. 6 Abs. 1 Satz 1 lit. b DS-GVO). Auch die Interessenabwägung des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO dürfte in der Regel zugunsten der schutzwürdigen Interessen der Mieter ausfallen.

Denn die §§ 22 Abs. 9 SGB II und 36 SGB XII sehen vor, dass (erst) das Gericht, bei dem eine Räumungsklage eingereicht wird, den zuständigen Sozialleistungsträger informiert. Vermieter tragen zwar häufig vor, dieser Zeitpunkt sei verspätet. Allerdings ist dies vornehmlich durch eigennützige wirtschaftliche Erwägungen begründet. Das Interesse der Vermieter, frühzeitig Mieteinnahmen und den Fortbestand des Mietverhältnisses zu stabilisieren, um den Aufwand der Mahnungen, Vollstreckungen, Räumung und neuen Mietersuche zu vermeiden, überwiegt regelmäßig nicht das Selbstbestimmungsrecht der Betroffenen, frei entscheiden zu können, ob, wann, in welchem Umfang und ggf. bei welchem (freien) Träger sie Hilfsangebote in Anspruch nehmen. Dabei muss auch berücksichtigt werden, dass nicht jeder relevante Zahlungsverzug zwangsläufig künftig in eine Wohnungslosigkeit münden muss.

Dem Vermieter bleibt es unbenommen, betroffenen Personen Informationsmaterial zur Verfügung zu stellen und damit auf Hilfsangebote und die zuständigen Träger aufmerksam zu machen, oder auch Daten zu übermitteln, nachdem die Betroffenen zuvor informiert und freiwillig eingewilligt haben (vgl. Art. 7, Art. 4 Nr. 11 DS-GVO, ErwGr 32, 42 und 43).

Sollten neben der möglicherweise drohenden Wohnungslosigkeit weitere gefährdende Begleitumstände vorliegen (z. B. konkrete Verdachtsmomente auf Kindeswohlgefährdung, Verwahrlosung, Gesundheitsgefährdung, Straftaten), wäre die Erforderlichkeit einer Datenübermittlung ausschließlich an dafür zuständige Stellen im konkreten Einzelfall zu prüfen.

14.4.3 Übermittlung von Mieterdaten an Grundversorger

Im Berichtszeitraum stellte sich die Frage, ob Vermieter berechtigt sind, dem örtlichen Strom-Grundversorger bei Einzug eines neuen Mieters dessen Namen mitzuteilen. Als Hintergrund wurde geschildert, dass die Kosten der Stromversorgung in der jeweiligen Wohnung nach Ablauf einer Frist von sechs Wochen dem Vermieter in Rechnung gestellt werden würden, falls der neue Mieter innerhalb dieser Frist keinen Stromlieferungsvertrag abgeschlossen hat.

Nach § 38 EnWG kann der Grundversorger, wenn der Mieter zuvor keinen Stromliefervertrag abgeschlossen hat, mit der ersten Stromabnahme in der neu bezogenen

Wohnung die Energielieferung in Rechnung stellen. Kommt durch die Stromentnahme aufgrund einer so genannten Realofferte ein Vertrag gemäß § 2 Abs. 2 StromGVV mit dem Grundversorger zustande, ist der Kunde verpflichtet, dem Grundversorger die Entnahme von Elektrizität unverzüglich in Textform mitzuteilen. Zudem ist der Kunde verpflichtet, dem Grundversorger auf Anforderung (unter anderem) seinen Namen mitzuteilen (§ 2 Abs. 3 StromGVV). Zuweilen kommen jedoch die Kunden diesen Mitteilungspflichten nicht nach.

Als Rechtsgrundlage für die Übermittlung der Mieterdaten vom Vermieter direkt an den Grundversorger kommt wiederum Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Ein berechtigtes Interesse des Vermieters kann dann vorliegen, wenn er ohne die Übermittlung der Mieterdaten an den Grundversorger die Kosten des Stromverbrauchs des Mieters zu tragen hätte. Eine Rechtsgrundlage, die regelmäßig eine Haftung des Vermieters für den Fall vorsieht, dass der Mieter keine Mitteilung an den Grundversorger erteilt, ist jedoch nicht ersichtlich. Allerdings ist eine Übermittlung personenbezogener Daten auch zulässig, wenn dies für die Wahrung der Interessen eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Hier können die Interessen des Grundversorgers herangezogen werden. Dieser hat ein berechtigtes Interesse, den Namen desjenigen zu erfahren, der aufgrund seiner Realofferte den Stromliefervertrag durch die Stromentnahme hat zustande kommen lassen. Allerdings ist hier insbesondere das Interesse derjenigen Mieter am Unterbleiben der Übermittlung zu berücksichtigen, die ordnungsgemäß einen Vertrag mit einem Stromlieferanten ihrer Wahl abgeschlossen haben.

Vor diesem Hintergrund kommt eine rein vorsorgliche Datenübermittlung an den Grundversorger nicht in Betracht. Nur wenn Anhaltspunkte dafür bestehen, dass der Mieter keinen Stromliefervertrag abgeschlossen haben und auch seinen Mitteilungspflichten gegenüber dem Grundversorger nicht nachgekommen sein könnte, sind die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO erfüllt und folglich Mitteilungen der Mieternamen zulässig.

Als praktische Lösung hat der Landesbeauftragte vorgeschlagen, den Mieter z. B. bei Einzug darum zu bitten, dem Vermieter binnen vier Wochen zu bestätigen, dass ein Stromliefervertrag abgeschlossen wurde. Diese Bitte könnte zusammen mit der Information erfolgen, dass bei Ausbleiben dieser Bestätigung der Vermieter dem örtlichen Grundversorger den Namen des Mieters mitteilen würde.

14.5 Speicherung von Kfz-Kennzeichen auf Supermarkt-Parkplätzen

Den Landesbeauftragten erreichte eine Anfrage, ob Supermärkte Kennzeichen von Kraftfahrzeugen speichern dürfen, um gegen wiederholte Parkverstöße auf dem jeweiligen Supermarkt-Parkplatz vorgehen zu können.

In bestimmten Fällen kann gegen eine nicht erlaubte Benutzung von Parkflächen vorgegangen werden. Dies kann z. B. durch das Abschleppen von Fahrzeugen geschehen, wenn Personen, die nicht im Supermarkt einkaufen wollen, ihr Fahrzeug auf dem Supermarkt-Parkplatz abstellen, obwohl die Nutzung des Parkplatzes nur für Kunden gestattet ist (s. BGH, Urteil vom 5. Juni 2009, V ZR 144/08).

Wird ein Fahrzeug auf einem Supermarkt-Parkplatz im Bereich eines privaten Halteverbotsschildes abgestellt, kann es zulässig sein, von der verantwortlichen Person die Kosten für anwaltliche Beratung und Hilfe sowie die Abgabe einer Unterlassungserklärung zu verlangen (s. BGH, Urteil vom 21. September 2012, V ZR 230/11).

In solchen oder ähnlichen Fällen kann es nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig sein, Kfz-Kennzeichen zur Verfolgung der rechtlichen Belange des Supermarktes zweckgebunden zu verarbeiten. Bei der Interessenabwägung gem. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO spielt es vor allem eine Rolle, ob der gestattete Umfang der Parkplatzbenutzung (z. B. durch Aushang oder Beschilderung) für jedermann erkennbar war.

14.6 Datenschutz bei Building Information Modeling

Mehrfach wurde der Landesbeauftragte gebeten, im Rahmen von Vorträgen und Interviews zum Datenschutz bei der Anwendung der Methode des Building Information Modeling (BIM) Stellung zu nehmen.

Der Begriff des „Building Information Modeling“ (deutsch: Bauwerksdatenmodellierung) beschreibt eine Methode der Planung, Ausführung und Bewirtschaftung von Gebäuden und anderen Bauwerken mit Hilfe elektronischer Datenverarbeitung. Als digitale Plattform führt BIM alle relevanten Daten, Pläne, Baufortschritte und Akteure zusammen und kann den gesamten Lebenszyklus eines Bauprojekts digital abbilden, von den ersten Entwürfen eines Bauwerks, der Durchführung der Baumaßnahmen bis hin zum Betrieb und Rückbau des Bauwerks. BIM vernetzt die Beteiligten am gesamten Bauprozess. Jeder Projektbeteiligte hat Zugriff auf die Daten – ob Vollzugriff oder eingeschränkt kann bzw. muss individuell festgelegt werden.

BIM ist ein Beispiel für den Digitalisierungsfortschritt in der Wirtschaft. Dieses Thema gehört in eine Novellierung der Digitalen Agenda des Landes. Datenschutz trägt zum Gelingen solcher Projekte bei. Der Landesbeauftragte hat mehrfach betont, dass der Datenschutz den BIM-Projekten nicht entgegensteht; allerdings sind dessen Regelungen zu beachten.

Dies gilt insbesondere deshalb, weil im Rahmen von BIM über zahlreiche natürliche Personen deren personenbezogene Daten verarbeitet werden. Zu den betroffenen Personen gehören z. B. Bauherren, Manager, Koordinatoren, Ingenieure, Statiker, Architekten, Bauleiter, Zeichner, Handwerker, Grundstückseigentümer, Nutzer sowie die am Projekt beteiligten Mitarbeiter der Unternehmen.

Zu diesen Personenkreisen werden eine Fülle von Einzeldaten verarbeitet. Dies sind Kontaktdaten, berufliche Qualifikationen und Spezialisierungen, Standortdaten, zahlreiche Projekt- und Kalendereinträge sowie personenbezogene Daten, die aufgrund der Bewirtschaftung zustande kommen.

Für diese umfangreichen Verarbeitungen sind insbesondere folgende datenschutzrechtliche Aspekte zu beachten:

- Als Rechtsgrundlage für Verarbeitung personenbezogener Daten kommt insbesondere Art. 6 Abs. 1 Satz 1 lit. b DS-GVO in Betracht. Die Verarbeitung

personenbezogener Daten von nicht am Vertrag Beteiligten kann auf Art. 6 Abs. 1 Satz 1 lit. f DS-GVO gestützt werden, soweit nicht deren Interessen oder Grundfreiheiten und Grundrechte überwiegen. Soweit die Verarbeitung im BIM-Projekt öffentlichen Interessen dient, kann die Verarbeitung auf der Grundlage des Art. 6 Abs. 1 Satz 1 lit. e DS-GVO erfolgen. Bei allen genannten Vorschriften ist zu beachten, dass nur die personenbezogenen Daten verarbeitet werden, die für die Durchführung des BIM-Projektes wirklich erforderlich sind. Dies kann eine detaillierte Prüfung erfordern. Die Zugriffsrechte der Beteiligten sind auf das für ihre Aufgabe erforderliche Maß zu beschränken. Es darf nur Software genutzt werden, mit der die entsprechende Datensparsamkeit verwirklicht werden kann, Art. 25 Abs. 1 DS-GVO. Soweit möglich, sollten personenbezogene Daten pseudonymisiert werden.

- Betroffene Personen müssen über die Verarbeitung ihrer Daten informiert werden. Gerade bei größeren Projekten kann es sinnvoll sein, die nach Art. 12 bis 14 DS-GVO erforderlichen Informationen durch einen zentralen Koordinator erarbeiten zu lassen. Zu informieren sind insbesondere Geschäftspartner als natürliche Personen, deren Beschäftigte, aber gegebenenfalls auch am Projekt Unbeteiligte (z. B. Grundstückseigentümer, deren Grundstücksdaten gerade im Rahmen von großen Baumaßnahmen – wie dem Straßenbau – verarbeitet werden). Auch die weiteren Betroffenenrechte (Art. 15 bis 21 DS-GVO) müssen beachtet werden.

- Die Zwecksetzung von BIM macht es erforderlich, eine Fülle von Arbeitsschritten und -ergebnissen, die einzelnen Mitarbeitern zugeordnet werden können, automatisiert zu protokollieren. Mitarbeiterbezogene Daten dürfen allerdings nur insoweit protokoliert und genutzt werden, als dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Dies ist dann der Fall, wenn diese Daten für die Planung, Ausführung und Bewirtschaftung im Rahmen des BIM benötigt werden. Hier ist insbesondere die Implementierung von Rollenkonzepten mit dem Ziel, den Personenbezug der protokollierten Daten auf ein Mindestmaß zu beschränken, zu prüfen. Die Nutzung der protokollierten mitarbeiterbezogenen Daten kann durchaus zu Kontrollzwecken oder zur Qualitätssicherung erfolgen; allerdings ist ein unverhältnismäßiger Überwachungsdruck für die Beschäftigten zu vermeiden.

- Bei mehreren beteiligten Unternehmen ist zu klären, wer die datenschutzrechtliche Verantwortung trägt. Verantwortlich ist immer derjenige, der die Zwecke und Mittel zur Verarbeitung personenbezogener Daten festlegt. Eine gemeinsame Verantwortung mehrerer Unternehmen kann auch vorliegen, wenn zwar einzelne Beteiligte für bestimmte Teile bzw. Phasen einer Verarbeitung getrennt verantwortlich sind, jedoch die Daten auf einer gemeinsamen Plattform zusammentragen. Aus einer gemeinsamen Verantwortung folgt, dass die Verantwortlichen gemäß Art. 26 DS-GVO in transparenter Weise festlegen, wer von ihnen welche der in der DS-GVO geregelten Verpflichtungen, insbesondere die Informationspflichten nach Art. 13 und 14 DS-GVO, erfüllt.

- An BIM-Projekten beteiligte Verantwortliche und Auftragsverarbeiter müssen ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO führen. Dies gilt auch für kleine Unternehmen (z. B. kleine Ingenieurbüros), wenn sie

aufgrund der Projektbeteiligung regelmäßig personenbezogene Daten verarbeiten.

- Im Falle der Auftragsverarbeitung (z. B. IT-Wartung, Cloud-Computing, Nutzung von Rechenzentren, Datenträgerentsorgung) ist gem. Art. 28 DS-GVO ein Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter abzuschließen.

- Gerade bei Großprojekten mit vielen Beteiligten und Beschäftigten sollte geprüft werden, ob eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO durchzuführen ist. Diese ist immer dann erforderlich, wenn eine Form der Verarbeitung personenbezogener Daten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Erforderlichkeit einer Datenschutz-Folgenabschätzung liegt bei BIM-Großprojekten sehr nahe.

- Schon im Hinblick auf die vielen sachbezogenen Daten, aber ohnehin in Bezug auf die umfangreiche Verarbeitung personenbezogener Daten, ist für BIM-Plattformen und die damit verbundene digitalisierte Nutzung die Beachtung der Grundsätze der Informationssicherheit unabdingbar (vgl. Art. 25, 32 DS-GVO).

Wie der Datenschutz einzuhalten ist, sollte schon bei der Projektvorbereitung thematisiert werden. Gerade bei Großprojekten ist es ratsam, einen Beauftragten einzusetzen, der den Datenschutz im BIM-Projekt insgesamt koordiniert.

14.7 Energieverbrauchsdaten auf Postkarten

Den Landesbeauftragten erreichten mehrere Beschwerden über Postkarten eines Energienetzbetreibers, mit denen dieser die Energieverbraucher um Ablesung und Übermittlung ihrer Verbrauchswerte bat. Auf diesen Postkarten waren neben den Namen und den vollständigen Anschriften der jeweiligen Anschlussinhaber die Zählernummer und Lieferstelle sowie ein sog. QR-Code aufgedruckt. Beim Nutzen dieses QR-Codes, z. B. mithilfe eines handelsüblichen Smartphones, wird eine Internetseite mit einer Eingabemaske aufgerufen, in der u. a. die Felder „Letzte Ablesung“ und „Letzter Zählerstand“ mit den bei dem Netzbetreiber vorhandenen Daten vorausgefüllt waren. Die weiteren Felder „Neues Ablesedatum“ und „Neuer Zählerstand in kWh“ waren für die Eingabe durch den Anschlussinhaber vorgesehen. Zudem war, sofern bekannt, die E-Mail-Adresse des Kunden ersichtlich. Eine Zugriffsbeschränkung, z. B. mittels Passwort, war nicht vorhanden.

Auf Anfrage des Landesbeauftragten hatte das Unternehmen zunächst dargelegt, dass derartige Postkarten an alle Kunden versandt wurden. Durch zusätzliche Sicherheitsmaßnahmen werde das Risiko des Missbrauchs des QR-Codes durch Unbefugte reduziert (z. B. begrenzte Gültigkeit des QR-Codes und zusätzliche Plausibilitätsprüfungen zur Missbrauchsprävention). Zudem sei zu beachten, dass auch Postkarten unter das Briefgeheimnis des Art. 10 GG und unter das Postgeheimnis im Sinne von § 39 PostG und § 206 StGB fallen. Inhaber oder Beschäftigte von Unternehmen, die geschäftsmäßig Postdienste erbringen, machen sich bei Verletzungen des Postgeheimnisses strafbar.

Die Maßnahmen und Begründungen reichten dem Landesbeauftragten jedoch nicht aus. Insbesondere war die Vertraulichkeit nach Art. 32 Abs. 1 lit. b DS-GVO nicht in ausreichendem Maße gewährleistet, da jeder, der den QR-Code mit seinem Smartphone (unberechtigterweise) nutzen würde, z. B. den Zählerstand hätte ablesen und einen neuen fingierten Zählerstand eintragen können. Im Ergebnis der Beratung teilte der Energienetzbetreiber mit, auf den Postkarten sowie in dem jeweiligen Online-Formular nach Aufruf des QR-Codes künftig die Zählernummer sowie die E-Mail-Adresse teilweise unkenntlich zu machen. Diese Änderungen bewertete der Landesbeauftragte als erforderlich, aber auch ausreichend, um die Anforderungen der Art. 25 und 32 DS-GVO zu erfüllen.

15 Videoüberwachung

Wie auch in den letzten Berichtszeiträumen stellt die Kontrolle der Verarbeitung personenbezogener Daten durch Videoüberwachung einen Schwerpunkt der Tätigkeit des Landesbeauftragten dar. Fast jede fünfte Beratung und Beschwerde im aktuellen Berichtszeitraum bezog sich auf die Videoüberwachung; damit setzte sich der Trend der vorhergehenden Berichtszeiträume fort.

Leider wurden die Grenzen einer zulässigen Videoüberwachung in den geprüften Fällen häufig überschritten. Vermehrt wurden folgende Verstöße festgestellt:

- Überschreitung des zulässigen Erfassungsbereiches und der zulässigen Speicherfristen,
- Heranziehung der Einwilligung als Rechtsgrundlage, obwohl die rechtlichen Voraussetzungen für die Einwilligung nicht vorlagen (insbesondere in Beschäftigtenverhältnissen),
- fehlende oder unzureichende Erfüllung der Informationspflichten,
- unzulängliche Dokumentation, keine oder nicht ausreichende Führung des Verzeichnisses der Verarbeitungstätigkeiten.

15.1 Rechtsgrundlage für nichtöffentliche Verantwortliche

Bereits in seinem XIII./XIV. Tätigkeitsbericht (Nr. 14.1.1) wies der Landesbeauftragte darauf hin, dass die Verarbeitung personenbezogener Daten mithilfe der Videoüberwachung durch nichtöffentliche Stellen generell nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu beurteilen ist.

Infolge einer Initiative aus dem Kreis der deutschen Aufsichtsbehörden befasste sich auch der EDSA mit Fragen der Anwendung der DS-GVO für die Videoüberwachung. In dessen Leitlinien 3/2019 wird einleitend darauf hingewiesen, dass Videogeräte in vielen Lebensbereichen auf den Einzelnen einen zusätzlichen Druck ausüben und die Auswirkungen auf den Datenschutz massiv sind (Guidelines 3/2019 on processing of personal data through video devices, adopted on 29 January 2020)[19]. Die

[19] https://lsaurl.de/edpb1903

Leitlinien beschreiben den Anwendungsbereich der DS-GVO und insbesondere die Rechtsgrundlagen der Videoüberwachung. Wichtigste allgemeine Rechtsgrundlage ist Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Zusätzlich muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) mithilfe von Videotechnik eine der Voraussetzungen des Art. 9 Abs. 2 DS-GVO erfüllt sein. Dies hat zur Folge, dass ein Einzelhändler, der in seinem Geschäft ein Gesichtserkennungssystem nutzen will, um seine Werbung an Einzelpersonen anzupassen, einer ausdrücklichen Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO bedarf. Auch wird darauf verwiesen, dass nach Art. 35 Abs. 3 lit. c DS-GVO eine Datenschutz-Folgenabschätzung erforderlich ist, wenn die Videoüberwachung eine systematische Überwachung eines öffentlich zugänglichen Bereichs in großem Maßstab darstellt. Dagegen fallen z. B. aus touristischen Gründen gefertigte Videoaufnahmen, die nur engen Freunden und der Familie gezeigt werden sollen, nicht unter das Regelwerk der DS-GVO.

Schon im XIII./XIV. Tätigkeitsbericht (Nr. 14.1.2) hat sich der Landesbeauftragte kritisch mit der Regelung des § 4 BDSG als Rechtsgrundlage befasst. § 4 Abs. 1 BDSG enthält eine besondere Gewichtung von Sicherheitsinteressen. Diese Vorschrift ist nach Auffassung des Bundesverwaltungsgerichts bei einer Videoüberwachung durch nichtöffentliche Stellen für private Zwecke nicht anwendbar (Urteil vom 27. März 2019, Az. 6 C 2/18, NJW 2019, 2556). Die Videoüberwachung sei allein an Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu messen. Der Landesbeauftragte begrüßt diese Klarstellung. Nach dieser Vorschrift ist die Videoüberwachung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Ergänzend stellt das Gericht fest, dass Art. 6 Abs. 1 Satz 1 lit. e DS-GVO für Privatpersonen (d. h. nichtöffentliche Stellen) nur dann als Rechtsgrundlage für die Videoüberwachung in Betracht komme, wenn ihnen die Befugnis, auf personenbezogene Daten zuzugreifen, im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt übertragen ist. Eine Privatperson könne sich nicht zum Sachwalter des öffentlichen Interesses erklären. Insbesondere sei sie nicht neben oder gar anstelle der Ordnungsbehörden zum Schutz der öffentlichen Sicherheit berufen. Zum Schutz individueller Rechtsgüter – der eigenen oder der von Dritten – könne sie keine öffentlichen Interessen, sondern nur private verfolgen. Im Falle der Videoüberwachung zur Verhinderung von Straftaten sei es zudem erforderlich, dass in Bezug auf die beobachteten Räume eine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage bestehe. Da in dem zu prüfenden Sachverhalt hierzu durch die Verantwortliche keine ausreichenden Angaben getätigt wurden, war die Livebeobachtung von Empfangs- und Wartebereich in einer Zahnarztpraxis unzulässig.

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 Informatio-

nen 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 berechtigte Interessen im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO dar, ebenso wie z. B. die Feststellung von unberechtigtem 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 unberechtigtem 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 berechtigte 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 milderen 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.

15.3 Videoüberwachung an Tankstellen

Bereits im vorletzten Berichtszeitraum hatte sich der Landesbeauftragte mit Fragen der Zulässigkeit der Videoüberwachung an Tankstellen befasst (XIII./XIV. Tätigkeitsbericht, Nr. 14.1.7). Im aktuellen Berichtszeitraum stellte er erneut ungenügende Hinweise zu Videoüberwachungen im Bereich von Zapfsäulen fest. Tankstellenbetreiber wurden auf notwendige Korrekturen hingewiesen. Zudem waren vom Mineralölwirtschaftsverband e. V. Fragen zur Kennzeichnung der Videoüberwachung an die DSK herangetragen worden.

Rechtsgrundlage für die Erfüllung der Informationspflichten im Falle der Videoüberwachung ist Art. 13 DS-GVO. Diese Vorschrift gibt in den Absätzen 1 und 2 einen umfangreichen Katalog von Angaben vor, über die bereits zum Zeitpunkt der Erhebung zu informieren ist. Zwar enthält § 4 Abs. 2 BDSG eine Formulierung, nach der zum frühestmöglichen Zeitpunkt lediglich der Umstand der Beobachtung, der Name und die Kontaktdaten des Verantwortlichen erkennbar zu machen sind. Diese Vorschrift kann nach Ansicht der Aufsichtsbehörden jedoch nicht so ausgelegt werden, dass sie die Informationspflichten der DS-GVO einschränkt. Zwar können die Informationspflichten durch nationales Recht beschränkt werden, wenn die Voraussetzungen des Art. 23 Abs. 1 DS-GVO erfüllt sind. Dies ist jedoch nur dann der Fall, wenn die Beschränkung für eine der in Art. 23 Abs. 1 lit. a bis j DS-GVO benannten Ziele erforderlich ist. Eine generelle Beschränkung der Informationspflichten – wie auch der Betroffenenrechte – ist nicht zulässig.

Die über § 4 Abs. 2 BDSG hinausgehenden Informationspflichten des Art. 13 DS-GVO sind daher in Gänze zu erfüllen. Dabei können die von den Datenschutzbehörden empfohlenen Muster für ein „vorgelagertes“ Hinweisschild und eine umfassende (nachgelagerte) Information als Aushang verwendet werden. Diese Muster sind auf der Homepage des Landesbeauftragten veröffentlicht.[20] Hinsichtlich der Angabe der Kontaktdaten des betrieblichen Datenschutzbeauftragten genügt die Angabe der Funktion, der Name ist nicht zwingend anzugeben. Die Zwecke der Datenverarbeitung können stichwortartig, jedoch nicht zu plakativ (vgl. Art. 12 Abs. 7 DS-GVO) angegeben werden. Die Stichworte müssen allerdings dem Ziel der Transparenzpflicht aus Art. 5 Abs. 1 lit. a DS-GVO, den Betroffenen über den Zweck der Videoüberwachung hinreichend konkret zu informieren, gerecht werden.

Zur Verhinderung von Auffahrunfällen oder Staus bei der Zufahrt zur Tankstelle wird eine Reduktion der Hinweispflichten auf ein während der Zufahrt gut sichtbares Piktogramm als vertretbar erachtet. An den Zapfsäulen reicht das „vorgelagerte“ Hinweisschild, während die vollständige Datenschutzinformation (durch den umfassenden Aushang) im oder am Kassenraum erfolgen könnte. Es bleibt dem Verantwortlichen natürlich unbenommen, die umfassende Information bereits an den Zapfsäulen anzubringen.

Diese Maßgaben wurden dem Mineralölwirtschaftsverband e. V. mitgeteilt. Er wurde ferner darauf hingewiesen, dass das Befahren eines erkennbar videoüberwachten Bereichs keine Einwilligung hinsichtlich der Videoüberwachung darstellt, da die betroffene Person nicht unmissverständlich bekundet, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Rechtmäßigkeit der Videoüberwachung richtet sich damit regelmäßig nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO.

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

[20] https://lsaurl.de/VideoInfo

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.

16 Sanktionen

16.1 Verwaltungs- und Bußgeldverfahren

Der Landesbeauftragte ist im Rahmen seiner aufsichtsbehördlichen Verpflichtungen neben Beratungstätigkeiten gehalten, Datenschutzverstöße nicht nur zu beseitigen, sondern ggf. auch zu sanktionieren. Wenn in weniger gravierenden Fällen schnell Abhilfe geleistet wird, der Verstoß also beseitigt ist und für die Zukunft keine erneute Datenschutzverletzung zu befürchten ist, kann dies zu einem Absehen von einem Sanktionsverfahren führen. Ansonsten ist aber zu berücksichtigen, dass die Verhängung von Geldbußen gem. Art. 83 Abs. 1 DS-GVO gerade einer wirksamen Durchsetzung des Rechts dienen soll.

Grundsätzlich haben aufsichtsbehördliche Maßnahmen in einem Verwaltungsverfahren Vorrang vor einer Sanktionierung (Art. 58 DS-GVO), da es dabei um die Beseitigung von Datenschutzverstößen für die Zukunft geht. Dagegen wirken Sanktionsmaßnahmen gegen Verstöße in der Vergangenheit. Die Kooperationspflichten des Verantwortlichen im aufsichtsbehördlichen Verwaltungsverfahren zwingen zur Mitwirkung bei der Sachverhaltsaufklärung. Für den Fall, dass sich in dem Verwaltungsverfahren ein Anfangsverdacht bzgl. einer Ordnungswidrigkeit nach Art. 83 DS-GVO ergeben könnte, wird der Verantwortliche bereits frühzeitig nach § 40 Abs. 4 BDSG über sein Aussageverweigerungsrecht belehrt. Nur dann können die trotzdem gemachten Angaben im Bußgeldverfahren verwendet werden.

Juristische Personen können nach Art. 4 Nr. 7 DS-GVO ebenso wie natürliche Personen Verantwortliche und damit Adressaten von Abhilfemaßnahmen oder Bußgeldbescheiden sein. Nach h. M. haben juristische Personen vertreten durch ihre Organe im Verwaltungsverfahren nur partielle Schweigerechte. Dagegen sind sie im Ordnungswidrigkeitsverfahren aufgrund Art. 6 Abs. 1 EMRK den natürlichen Personen (nahezu) gleichgestellt. Die Belehrung über das Aussageverweigerungsrecht in ei-

[21] https://lsaurl.de/inhin

nem Verwaltungsverfahren erstreckt sich daher auch auf den Schutz der betroffenen juristischen Person.

Dauert ein datenschutzrechtlicher Verstoß nicht mehr an oder ist er beseitigt, kann, wenn ein entsprechender Anfangsverdacht besteht, ein Bußgeldverfahren auch direkt, d. h. ohne vorgeschaltetes Verwaltungsverfahren, eingeleitet werden. Nach ErwGr 148 kann unter anderem in geringfügigen Fällen anstelle einer Geldbuße eine Verwarnung ausgesprochen werden.

Einen besonderen Blick verdient die Datenpannenmeldung nach Art. 33 DS-GVO: Diese muss unverzüglich und möglichst innerhalb von 72 Stunden erfolgen und Informationen zur Verletzung des Schutzes personenbezogener Daten einschließlich Art, Kategorie, Zahl, Folgen und zu ergriffenen Maßnahmen enthalten. Erfolgt die Meldung nicht rechtzeitig, ist eine Begründung für die Verzögerung beizufügen. Art. 33 DS-GVO zwingt also den Verantwortlichen unter Androhung einer Geldbuße, die Meldung notfalls verspätet abzugeben, auch wenn das Risiko besteht, dass er sich selbst belastet.

Nach §§ 42 Abs. 4, 43 Abs. 4 BDSG unterliegt jedoch die Meldung einem Verwertungsverbot, d. h. sie darf in einem Straf- oder Bußgeldverfahren nicht verwendet werden. Allerdings ist die Reichweite dieser Vorschriften umstritten.

Die Selbstbelastungsfreiheit untersagt, jemanden zu zwingen, sich durch seine Aussage selbst zu bezichtigen oder an seiner Überführung mitzuwirken; das Recht auf ein faires Verfahren verbietet einen Zwang, zu der eigenen Verurteilung aktiv beitragen zu müssen. Somit sind alle von der Datenpannenmeldung direkt umfassten Elemente von einer Ahndung im Bußgeldverfahren ausgeschlossen: Dies schließt den Verstoß, der zur Panne geführt hat, als auch ggf. unvollständige oder mit Fehlern behaftete Informationen und auch die Verspätung der Meldung und deren Begründung ein.

Im Übrigen ist das Verwertungsverbot eng auszulegen. Wenn es im Ergebnis nur um den gemeldeten konkreten Verstoß geht, dann kann z. B. die Meldung über eine Datenpanne aufgrund mangelhafter technisch-organisatorischer Maßnahmen trotzdem zu einem Bußgeld führen, wenn sich bei der Überprüfung des Vorfalls durch die Aufsichtsbehörde weitere datenschutzwidrige Zustände herausstellen. Beispielsweise kann dies gegeben sein, wenn die Daten bereits vorher hätten gelöscht werden müssen, kein Datenschutzbeauftragter bestellt war oder kein Verarbeitungsverzeichnis geführt wurde. Darüber hinaus kann die gemeldete Datenschutzverletzung sanktioniert werden, wenn sie der Behörde auch ohne die Meldung z. B. durch eine Beschwerde oder Eingabe bekannt geworden ist.

16.2 Ahndung von Datenschutzverstößen und Bemessung der Bußgeldhöhe

Der Landesbeauftragte errichtete eine Teileinheit, die datenschutzrelevante Vorgänge unter ordnungswidrigkeitsrechtlichen Aspekten untersucht und Bußgeldverfahren durchführt. Kenntnis von bußgeldrelevanten Vorgängen erhält diese Stelle von dem für das Verwaltungsverfahren zuständigen Fachreferat, durch Beschwerden betroffener Personen, von anderen hinweisgebenden Personen sowie durch Anzeigen von Staatsanwaltschaften und Polizei.

Anonyme Anzeigen werden zunächst grundsätzlich mit Vorsicht behandelt und nur beachtet, wenn schlüssige Hinweise auf Datenschutzverstöße vorgebracht werden. In diesem Zusammenhang ist auf die „Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ zu verweisen, die bis zum 17. Dezember 2021 in deutsches Recht umzusetzen ist und die ausdrücklich auch auf die Meldung von Datenschutzverstößen Anwendung finden soll.

Für Verstöße, die mit einem Bußgeld gemäß Art. 83 Abs. 4 bis 6 DS-GVO geahndet werden sollen, gilt nach § 41 Abs. 1 BDSG das OWiG sinngemäß. Über § 46 Abs. 1 OWiG findet die StPO entsprechende Anwendung. Der Landesbeauftragte hat damit gemäß § 46 Abs. 2 OWiG als Verfolgungsbehörde im Bußgeldverfahren im Wesentlichen dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Hierzu zählen unter anderem die Vernehmung von Zeugen, die auch zwangsweise durchgesetzt werden kann, sowie die Erwirkung und der Vollzug von Durchsuchungs- und Beschlagnahmebeschlüssen.

In 2019 wurden 16 Bußgeldverfahren eingeleitet. Acht Verfahren (teilweise noch aus 2018) wurden mit der Festsetzung eines Bußgeldes rechtskräftig abgeschlossen und drei Verfahren wurden eingestellt. Insgesamt wurden Bußgelder i. H. v. 12.620 Euro rechtskräftig verhängt:

Tatbestände	Bußgelder insgesamt
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Datenverarbeitung zu fremden Zwecken	160 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässiger Versand von E-Mails mit offenem Verteiler	2.500 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässiger Versand von Werbe-E-Mails	1.450 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässiger Versand einer unverschlüsselten E-Mail mit sensiblen personenbezogenen Daten an einen unberechtigten Empfänger	3.700 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Videoüberwachung des öffentlichen Straßenraums	1.300 Euro
Art. 83 Abs. 5 lit. b i. V. m. Art. 15, 12 DS-GVO Verspätete Auskunftserteilung	2.800 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 31 DS-GVO Unzureichende Zusammenarbeit mit der Aufsichtsbehörde	710 Euro

Für die Bemessung der Höhe einer Geldbuße gilt, dass sie in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein soll (Art. 83 Abs. 1 DS-GVO). Dazu werden die Umstände des Einzelfalls bewertet (Art. 83 Abs. 2 DS-GVO). Schwere und Dauer des Verstoßes und der Umstand, ob der Verstoß aus grober Unachtsamkeit oder sogar vorsätzlich begangen wurde, spielen eine große Rolle. Ebenso ist auch die Kooperation mit der Aufsichtsbehörde bedeutsam. Auch sind die Auswirkungen des Verstoßes entscheidend, d. h., ob eine erhebliche Anzahl von Personen betroffen ist und/oder eine erhebliche Datenmenge. Auch wird die Kategorie der betroffenen personenbezogenen Daten (ggf. sensible Daten wie Gesundheitsdaten) berücksichtigt. Relevant ist ferner, ob es sich um einen ersten Verstoß handelt oder um eine Wiederholungstat.

Für formal-rechtliche Verstöße nach Art. 83 Abs. 4 DS-GVO können Bußgelder bis zu 10 Millionen Euro bzw. 2 % des weltweiten Konzernumsatzes eines Unternehmens verhängt werden. Für materiell-rechtliche Verstöße nach Art. 83 Abs. 5 DS-GVO gilt ein Bußgeldrahmen bis zu 20 Millionen Euro bzw. 4 % des weltweiten Konzernumsatzes eines Unternehmens.

Es existiert weder ein nationaler noch ein europäischer Bußgeldkatalog. Auf Bundes- und Länderebene wird an der Erstellung von bundeseinheitlichen Richtlinien für die Verhängung von Geldbußen gearbeitet. Ein erstes Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen wurde von der DSK am 14. Oktober 2019 beschlossen und anschließend auf ihrer Webseite veröffentlicht[22]. Basis für die Bußgeldzumessung ist danach ein Grundwert, der aufgrund des Umsatzes des betreffenden Unternehmens ermittelt wird. Je nach Schwere des Verstoßes wird der Grundwert mit Faktoren multipliziert. Danach werden be- oder entlastende Umstände des Einzelfalls in der Berechnung berücksichtigt. Auf europäischer Ebene arbeitet die Fachuntergruppe des EDSA „Taskforce Fining“ an einer europäischen Vereinheitlichung der Bußgeldpraxis.

16.3 Haftung von Unternehmen für Datenschutzverstöße ihrer Beschäftigten

Ein Unternehmen haftet als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO nicht nur, wenn die Geschäftsführung oder Organmitglieder Datenschutzrecht verletzen, sondern auch, wenn jede andere beschäftigte Person bei Ausführung ihrer Tätigkeiten gegen Datenschutzvorgaben verstößt (sog. funktionaler Unternehmensbegriff). Die Haftungsnormen der §§ 30, 130 OWiG für juristische Personen und Personenvereinigungen sind im Hinblick auf die Haftung für einen Verstoß durch andere beschäftigte Personen restriktiver als die DS-GVO. In der Verweisungsnorm des § 41 Abs. 1 BDSG wurden diese Paragraphen nicht ausgenommen. Unter Berücksichtigung des Anwendungsvorrangs der DS-GVO als EU-Recht müssen § 41 Abs. 1 BDSG und das OWiG sinngemäß so ausgelegt werden, dass die §§ 30, 130 OWiG keine Anwendung finden (s. die Entschließung der DSK vom 3. April 2019, **Anlage 2**). Sofern eine beschäftigte Person einen Verstoß im Rahmen ihrer beruflichen Tätigkeiten begeht und dabei eigene wirtschaftliche oder private Zwecke und Interessen verfolgt, haftet nicht das Unternehmen, sondern sie selbst als Verantwortliche (sog. Mitarbeiter-Exzess).

[22] https://lsaurl.de/dskpm

Anlagen

Anlage 1

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 1. April 2019[23]

Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich am 5. September 2018 zu dem (Weiter-)Betrieb von Facebook-Fanpages nach dem Urteil des EuGH vom 5. Juni 2018 geäußert. In ihrem Beschluss hat die Konferenz deutlich gemacht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25, 32 DSGVO.

Am 11. September 2018 veröffentlichte Facebook eine sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“. Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO. Insbesondere steht es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten" einräumen lassen will. Die von Facebook veröffentlichten Informationen stellen zudem 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. Vor diesem Hintergrund bekräftigt die Konferenz erneut die Rechenschaftspflicht der Fanpage-Betreiber (unabhängig von dem Grad der Verantwortlichkeit) und stellt fest:

1. Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführen, sondern durch andere gemeinsam mit ihnen Verantwortlichen durchführen lassen.

2. Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, sind Verantwortliche nicht in der Lage, zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestehen Zweifel, geht dies zulasten der Verantwortlichen, die es in der Hand haben, solche Verarbeitungen zu unterlassen. Der EuGH führt hierzu aus:

[23] Unter Enthaltung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

„Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Datenbefreien.“ (EuGH, C-210/16, Rn. 40).

3. Im Hinblick auf die Ausführungen zur „Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche“ sowie zur federführenden Aufsichtsbehörde (Punkt 4 in der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“) weist die Konferenz darauf hin, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für Fanpage-Betreiber nach der DSGVO richtet. Nach Art. 55 ff. DSGVO sind die Aufsichtsbehörden für Verantwortliche (wie z. B. Fanpage-Betreiber) in ihrem Hoheitsgebiet zuständig. Dies gilt unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Kohärenzmechanismen.

Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

Anlage 2

Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019 auf dem Hambacher Schloss[24]

Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!

Unternehmen haften im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse“), sind ausgenommen.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unternehmen generell im deutschen Recht so zu ändern, dass „die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden“. Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

---

[24] Gegen die Stimmen von Bayern und Baden-Württemberg

Anlage 3

Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019 auf dem Hambacher Schloss

Hambacher Erklärung zur Künstlichen Intelligenz

Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ [...].“[25]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken

[25] BT-Drs. 19/1982 zu 1., Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018;).

oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art.5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung

(Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u. a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung

und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art.32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art.35 DS-GVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DS-GVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutz-aufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

Anlage 4

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 23. April 2019

Keine Abschaffung der Datenschutzbeauftragten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Nach § 38 Bundesdatenschutzgesetz müssen z. B. Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.

Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutz-Grundverordnung bewährt.

Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.

Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

Anlage 5

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 12. September 2019

Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten!

Die Bundesregierung will die in der Verwaltung geführten Register modernisieren und plant in diesem Zusammenhang einen einfacheren Zugriff auf dort gespeicherte personenbezogene Daten. Nach Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) darf dieses Vorhaben nicht zur Einführung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren führen. Vielmehr muss der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten, Priorität haben. Ebenso wichtig ist es, den Bürgerinnen und Bürgern die besseren Dienstleistungen verbunden mit einer deutlich höheren Transparenz anzubieten.

Bundesregierung nimmt Modernisierung der Register in Angriff

Die Bundesregierung hat mit dem Onlinezugangsgesetz ein umfangreiches Digitalisierungsprogramm für die Verwaltung in Deutschland gestartet. Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten. Es sollen Nutzerkonten bereitgestellt werden, über die sich Nutzende für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.

In diesem Zusammenhang hat sich der Nationale Normenkontrollrat (NKR) für eine Modernisierung der deutschen Registerlandschaft ausgesprochen und empfohlen, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only“-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen und ein „Datencockpit“ einzurichten, bei dem die Bürgerinnen und Bürger alle staatlichen Datenflüsse im Auge haben können.
Die Einführung solcher Identifikationsnummern für Personen wird aktuell unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) von der Bundesregierung verfolgt. Der IT-Planungsrat hat in seiner 28. Sitzung am 12. März 2019 den vom BMI vorgelegten „Leitlinien für eine Modernisierung der Registerlandschaft“ zugestimmt sowie den „Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung“ zur Kenntnis genommen und das angestrebte Vorhaben begrüßt.

Datenschutzfreundliche und transparente Gestaltung für Bürgerinnen und Bürger

Bereits die Schaffung einheitlicher und verwaltungsübergreifender Personenkennzeichen bzw. Identifikatoren und einer entsprechenden Infrastruktur zum Datenaustausch bergen die Gefahr, dass personenbezogene Daten in großem Maße leicht

zusammengetragen, verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden könnten. Die Datenschutzkonferenz weist darauf hin, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat gefährdet das Persönlichkeitsrecht, da sie bei den Menschen zu einer vorauseilenden Anpassung ihres Verhaltens führen kann. Auch die Grundsätze der europäischen Datenschutz-Grundverordnung und deren Regelungen zur datenschutzgerechten Gestaltung setzen einheitlichen und verwaltungsübergreifenden Personenkennzeichen enge Grenzen und verlangen geeignete Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen.

Insbesondere im Hinblick auf die geplante Verwendung modernisierter Register für zukünftige Zensus-Erhebungen und geplante/modernisierte Zugriffsrechte der Sicherheitsbehörden bedarf es eines besonderen Schutzes der betroffenen Personen. Den hohen Risiken für das Recht auf informationelle Selbstbestimmung muss in einem umfassenden regulatorischen, vor allem aber technischen und organisatorischen Konzept begegnet werden. Nur so können die vom deutschen und europäischen Verfassungsrecht geforderten Garantien gewahrt werden.

Die Modernisierung der Register muss zwingend von Beginn an auch dafür genutzt werden, den Bürgerinnen und Bürgern die Nutzung der im Online-Zugangsgesetz vorgesehenen Dienstleistungen durch Nutzung einmal hinterlegter Daten zu erleichtern. Von besonderer Bedeutung ist es darüber hinaus, den Bürgerinnen und Bürgern ein im Vergleich zur gegenwärtigen Situation deutlich höheres Maß an Transparenz zu gewährleisten. Ein „Datencockpit“, wie es der NKR bereits vorgeschlagen hat, muss es den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welches Register welche Daten über sie vorhält, welche Behörden darauf zugegriffen haben und mit welchen anderen Daten diese verknüpft wurden. Gleichzeitig muss gewährleistet sein, dass ausschließlich den betroffenen Bürgerinnen und Bürgern der Zugriff möglich ist. Auf dieser Grundlage muss die Digitalisierung der Verwaltung dazu genutzt werden, das informationelle Machtgefälle zwischen Staat und Bürgerinnen und Bürgern weitgehend aufzuheben und ihnen die Inanspruchnahme ihrer Rechte deutlich zu erleichtern.

Dazu muss nach Auffassung der Datenschutzkonferenz die dezentrale Registerstruktur erhalten bleiben. Die Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern lehnt die Datenschutzkonferenz ab. Sie fordert alternative Methoden zur eindeutigen Identifizierung. Neben Abgleichen über den jeweiligen Datensatz des Registers kämen dafür allenfalls sektorspezifische Personenkennziffern in Betracht, die eine eindeutige Identifizierung erlauben, einseitigen staatlichen Abgleich von Daten verhindern, ein Höchstmaß an Transparenz beispielsweise durch ein Datencockpit ermöglichen, das Risiko von Missbrauch und Kompromittierung verringern und die Eindeutigkeit von Registern gewährleisten.

Anlage 6

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Auf der Grundlage der Hambacher Erklärung vom 03.04.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.

Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der DS-GVO formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegen-sätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

Anlage:

Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen[26]

[26] https://lsaurl.de/dskpopaki

Anlage 7

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking -und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.

So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking-und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie z.B. körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.

Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.

Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

- Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins – keinen eigenen Zugriff auf die weitergeleiteten Daten haben.

- Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Art. 9 Abs. 1, 2 Buchst. a Datenschutz-Grundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.

- Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.

- Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking-oder Analyse-Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

Anlage 8

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutz-Grundverordnung flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.

In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.

Der Einsatz von Informations-und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen unabhängig von ihrer Größe aufgrund der Datenschutz-Grundverordnung verpflichtet.

Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

Anlage 9

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.

Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.

Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierender Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Ausweitung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.

Angesichts einer fehlenden Rechtsgrundlage sieht die DSK in der geschilderten exzessiven Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung. Die DSK fordert die Polizeibehörden und Staatsanwaltschaften auf, die umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme für Zwecke der Strafverfolgung zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen einen Eingriff von erheblichem Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

Anlage 10

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2019

Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen

Zukünftig sollen nach einem Referentenentwurf zur Änderung des Rundfunkbeitragsstaatsvertrags (RBStV) regelmäßig alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt zur Sicherstellung der Aktualität des dortigen Datenbestandes übermittelt werden. Gemäß Art. 1 Ziffer 7 dieses Entwurfs des 23. Rundfunkänderungsstaatsvertrages vom 5. Februar 2019 zählen zu den Meldedaten neben Namen und gegenwärtiger und letzter Anschrift insbesondere auch Geburtstag, Titel, Familienstand sowie die genaue Lage der Wohnung.

Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war seinerzeit auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010). Die DSK stellte ihre Bedenken nur deshalb teilweise zurück, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Mit der nun vorgesehenen Regelung wären die - bereits damals zweifelhaften - Zusicherungen des Gesetzgebers, dass es sich bei den anlasslosen vollständigen Meldedatenabgleichen aus den Jahren 2013 und 2018 um einmalige Vorgänge handeln würde, endgültig hinfällig.

Gegen die geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs bestehen weiterhin grundlegende verfassungsrechtliche und datenschutzrechtliche Bedenken.

Ein solcher Abgleich stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und gerät in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO).

Bei einem vollständigen Meldedatenabgleich werden in großem Umfang personenbezogene Daten von Betroffenen, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen Beiträge gezahlt werden oder weil sie von der Beitragspflicht befreit sind, an die Rundfunkanstalten übermittelt und von diesen verarbeitet. Zudem werden auch Daten von all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die sich bereits bei der Landesrundfunkanstalt angemeldet haben und regelmäßig ihre Beiträge zahlen. Dabei betrifft der geplante Meldedatenabgleich mehr personenbezogene Daten, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, z. B. Doktorgrad und Familienstand (vgl. § 8 Abs. 4 RBStV). Es sollen also personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die nicht zur Beitragserhebung notwendig sind.

Die Meldedaten-Übermittlungsverordnungen der Länder bieten mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten bereits eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes des Beitragsservices auch bei Veränderungen der Meldesituation der Beitragsschuldnerinnen und Beitragsschuldner zu gewährleisten. Auch wenn die Meldebehörden in Einzelfällen eine Änderungsmitteilung unterlassen sollten, würde ein erneuter vollständiger Meldedatenabgleich in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Beitragsschuldner eingreifen, ohne dass dies durch andere Gesichtspunkte, etwa das Ziel der Gebührengerechtigkeit, gerechtfertigt wäre.

Die Landesrundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldedatenabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (vgl. Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019).

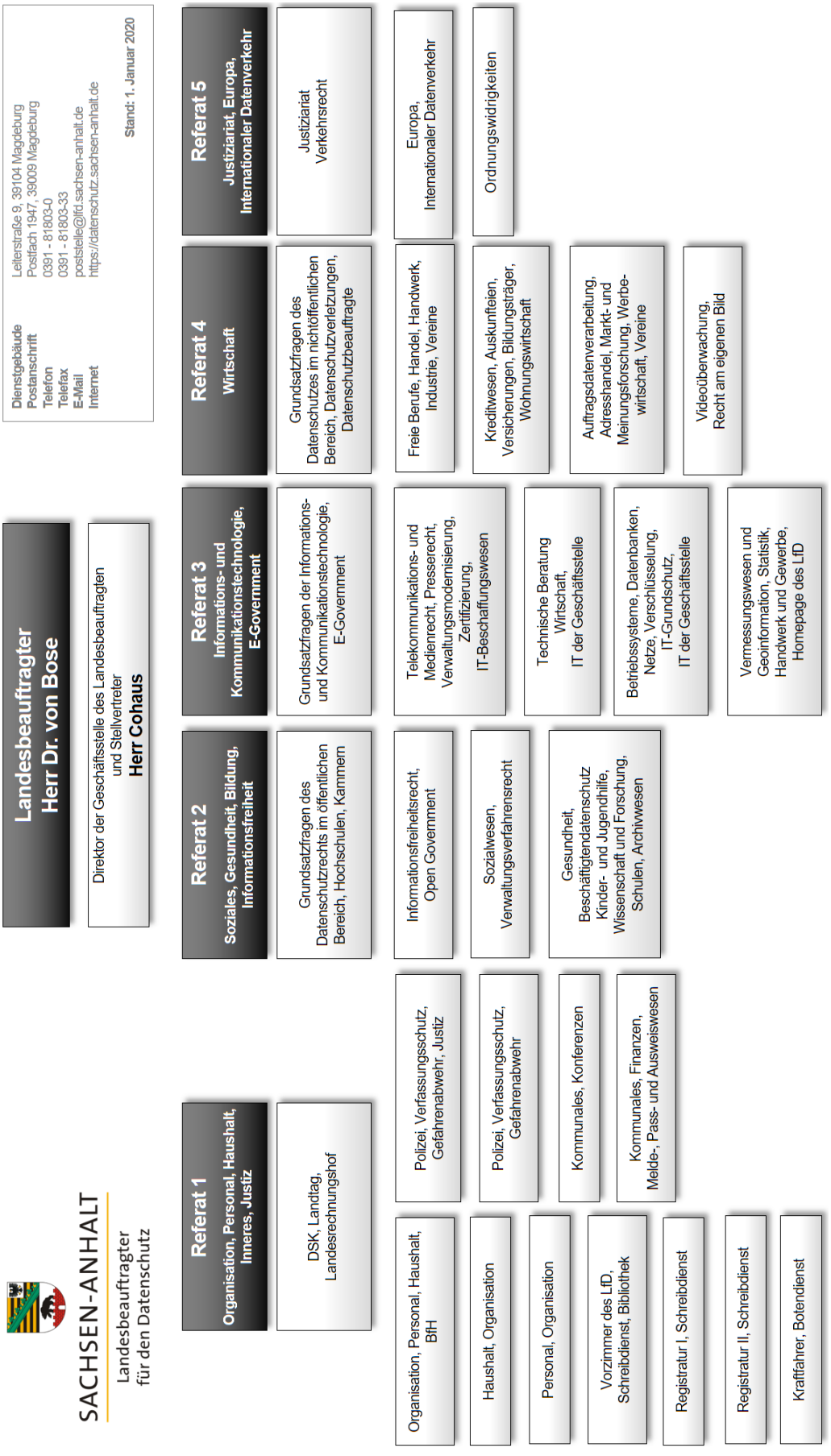
Die geplanten Regelungen berücksichtigen zudem die Maßstäbe der DS-GVO nicht ausreichend. Nationale Datenschutzvorschriften müssen aufgrund des Anwendungsvorrangs europäischer Verordnungen auf eine Öffnungsklausel der DS-GVO gestützt werden können. Art. 85 Abs. 2 DS-GVO ist nicht einschlägig, da die Datenverarbeitung zum Zweck des Einzugs des Rundfunkbeitrags nicht in dem Anwendungsbereich dieser Norm liegt. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e DS-GVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Mitgliedstaatliche Regelungen für die Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, dürfen danach eingeführt werden, wenn diese die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DS-GVO vorgibt. Hier bestehen erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.

Positiv hervorzuheben ist zwar, dass die bisherige Vermieterauskunft im Hinblick auf Mietwohnungen aus § 9 Abs. 1 Satz 2 und 3 RBStV gestrichen werden soll. Ebenso soll der Ankauf von Adressdaten von Privatpersonen ausdrücklich ausgeschlossen werden. Beide Datenverarbeitungen sind aus Sicht des Datenschutzes kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich eine weitaus umfassendere, datenschutzrechtlich ebenfalls sehr bedenkliche Möglichkeit der Datenerhebung geschaffen werden soll, die das praktische Bedürfnis der Vermieterauskunft und des Ankaufs privater Adressen ohnehin entfallen lässt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen.

Anlage 11

Organigramm



Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

J

W

Z