SACHSEN-ANHALT

XIII. / XIV. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Dieser Text entspricht der Landtagsdrucksache 7/3361

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Postfach 1947, 39009 Magdeburg

Telefon:	0391 81803 0
Fax:	0391 81803 33
Bürgertelefon:	0800 91531 90
Internet:	https://www.datenschutz.sachsen-anhalt.de
E-Mail:	poststelle@lfd.sachsen-anhalt.de
Dienstgebäude:	Leiterstraße 9, 39104 Magdeburg

Vorwort

Der XIII. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2015 bis zum 31. März 2017. Der XIII. Tätigkeitsbericht wird gemeinsam mit dem XIV. Tätigkeitsbericht (für einen verkürzten Zeitraum vom 1. April 2017 bis 5. Mai 2018) veröffentlicht, denn infolge der Europäischen Datenschutz-Grundverordnung (DS-GVO) ist bereits für das Jahr 2018 ein eigenständiger, jährlicher Tätigkeitsbericht neuen Typs auf europäischer Rechtsgrundlage zu erstellen. Der Landesbeauftragte nimmt entsprechend der Entscheidung des Landesgesetzgebers die neuen Aufgaben und Befugnisse gemäß der DS-GVO und der Europäischen Richtlinie für den Bereich von Polizei und Justiz (sog. JI-Richtlinie) seit 6. Mai 2018 wahr. Zu diesem Zeitpunkt endete die Verpflichtung zur Erstellung eines Tätigkeitsberichts alten Typs.

Bei einzelnen Beiträgen konnten noch darüber hinausreichende aktuelle Sachstände einbezogen (Redaktionsschluss: 31. Juli 2018) und Entwicklungen in Gesetzgebung und Rechtsprechung berücksichtigt werden. Insbesondere bei Themen aus dem Bereich der Wirtschaft und weiterer nichtöffentlicher Stellen werden auch Hinweise auf die neue Rechtslage nach DS-GVO gegeben.

Der Tätigkeitszeitraum war in besonderer Weise durch die Vorbereitung auf das neue europäische Recht geprägt, sowohl im Hinblick auf die Beratung des Gesetzgebers als auch der Rechtsanwender.

Mein besonders großer Dank gilt dafür meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle.

Der Datenschutzbericht dient nicht nur der Unterrichtung des Landtages, sondern auch der Information der Behörden, Unternehmen und anderer verantwortlicher Stellen sowie interessierter Bürgerinnen und Bürger. Im Anlagenteil sind insbesondere rechtspolitische Empfehlungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder aufgenommen.

Meine zweite Amtszeit endete im März 2017. Gemäß § 20 Abs. 2 Satz 2 DSG LSA bin ich verpflichtet, das Amt bis zur Bestellung eines Nachfolgers weiterzuführen; die Amtszeit gilt als entsprechend verlängert. Dieser Verantwortung habe ich mich gestellt, auch über das Frühjahr 2018 hinaus, als die Wahl meines Nachfolgers leider nicht gelang.

Magdeburg, den 18. September 2018

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

Inhaltsverzeichnis

Anlagenverzeichnis

Nationale Datenschutzkonferenz

Abkürzungsverzeichnis

A	
ABES	Asylbewerbermanagementsystem
AD	Active Directory (Verzeichnisdienst)
AES	Advanced Encryption Standard, ein symmetrisches Verschlüsselungsverfahren
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
AöR	Anstalt des öffentlichen Rechts
Art.	Artikel
ATDG	Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern
AufnG	Aufnahmegesetz
Az.	Aktenzeichen
Azure	Microsoft Azure ist eine Cloud-Computing-Plattform
B	
BbS-VO	Verordnung über Berufsbildende Schulen
BDSG	Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003 (BGBl I S. 66), zuletzt geändert durch Art. 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2131)
BDSG 2018	Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (BGBl. I S. 2097)
beA	besonderes elektronisches Anwaltspostfach
BeamtStG	Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern (Beamtenstatusgesetz)
beBPo	besonderes elektronisches Behördenpostfach
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMI	Bundesministerium des Innern, für Bau und Heimat
BPolG	Gesetz über die Bundespolizei
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestagsdrucksache
bzw.	beziehungsweise
C	
CA	Certificate Authority (Zertifizierungsstelle)
CC	Common Criteria (Evaluierungskriterien für IT-Sicherheit auf der Basis von ISO/IEC 15408)
CD	Compact Disc

CETA	Comprehensive Economic and Trade Agreement

D

DG LSA	Disziplinargesetz Sachsen-Anhalt
DLP	Data Leakage Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions, Erweiterungen des DNS-Protokolls zur Quellenauthentisierung
DS-GVO	Datenschutz-Grundverordnung, EU-Verordnung 2016/679, Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
DSAG LSA	Gesetz zur Ausfüllung der DS-GVO und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU, Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680
DSFA	Datenschutz-Folgenabschätzung
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DSK	Konferenz der unabhängigen Datenschutzbehörden 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 (JI-Richtlinie) sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes
DVD	Digital Versatile Disc
d. h.	das heißt

E

e²	Abkürzung für „ergonomisch-elektronisch“, siehe Nr. 8.2
ECDHE	Elliptic Curve Diffie-Hellman Exchange (verdeckte Passwortübertragung mittels Elliptischen Kurven)
EDSA	Europäischer Datenschutzausschuss
eGK	Elektronische Gesundheitskarte
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	Elektronische Identität
ERV	Elektronischer Rechtsverkehr
ErwGr	Erwägungsgrund
ESF	Europäischer Sozialfond
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EU DS-GVO	EU Datenschutz-Grundverordnung, siehe DS-GVO
EUREKA	Abkürzung für „EDV-Unterstützung für Rechtsgeschäftsstellen und Kanzleien sowie Richter- und Rechtspflegerarbeitsplätze“

EUREKA-Fach	Fachanwendung für die Arbeits-, Finanz-, Sozial- und Verwaltungsgerichtsbarkeit zur einheitlichen IT-Unterstützung
Eurostat	Statistisches Amt der Europäischen Union
EWR	Europäischer Wirtschaftsraum
E-ZensVorbG 2021	Entwurf eines Zensusvorbereitungsgesetzes 2021

F

FDR	Falldatei Rauschgift
ff	fortfolgende
FITKO	Föderale IT-Kooperation

G

GDIG LSA	Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt
GewO	Gewerbeordnung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
gGmbH	gemeinnützige GmbH
GKDZ-StV	Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts
GlüG LSA	Glücksspielgesetz des Landes Sachsen-Anhalt
GlüStV	Staatsvertrag zum Glücksspielwesen in Deutschland (Glücksspielstaatsvertrag)
GPS	Global Positioning System (Navigationssatellitensystem)
GVBl. LSA	Gesetz und Verordnungsblatt des Landes Sachsen-Anhalt
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)

H

HTTP	Hypertext Transfer Protocol („Hypertext-Übertragungsprotokoll“)
HTTPS	Hypertext Transfer Protocol Secure („sicheres Hypertext-Übertragungsprotokoll“)

I

IDS	Intrusion Detection System (Angriffserkennungssystem)
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
IMI	Internal Market Information System (Europäisches Binnenmarkt-Informationssystem)
IP	Internetprotokoll
ITN-LSA	Informationstechnisches Netz Land Sachsen-Anhalt
ITN-XT	Informationstechnisches Netz Sachsen-Anhalt „eXTended“ (erweitert)

ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization (Internationale Organisation für Normung)
i. S. d.	im Sinne des
IT	Informationstechnik
IT-PLR	IT-Planungsrat

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.
JVollzGB LSA	Justizvollzugsgesetzbuch Sachsen-Anhalt

K

KiFöG	Kinderförderungsgesetz
KONSENS	Koordinierung neue Softwareentwicklung der Steuerverwaltung
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie (Kunsturhebergesetz)
KV	Kassenärztliche Vereinigung
KVG	Kommunalverfassungsgesetz
KVSA	Kassenärztliche Vereinigung Sachsen-Anhalt

L

LBG LSA	Beamtengesetz des Landes Sachsen-Anhalt (Landesbeamtengesetz)
lit.	Buchstabe (lateinisch: littera)
LKA	Landeskriminalamt Sachsen-Anhalt
LPSA	Landesportal Sachsen-Anhalt (die Website www.sachsen-anhalt.de)
LT-Drs.	Landtagsdrucksache

M

Meld-DÜVO-LSA	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden in Sachsen-Anhalt
MF	Ministerium der Finanzen des Landes Sachsen-Anhalt
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MI	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt
MITM	Man in the Middle (Mann in der Mitte, Angriff auf eine Datenübertragung, bei der sich der Angreifer zwischen den Kommunikationspartnern befindet)
MJ	Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt

N

NAT	Network Address Translation (Netzwerkadressübersetzung)
NJW	Neue Juristische Wochenschrift
nPA	Neuer Personalausweis

O

o. a.	oben angegeben(e/es/er)
o. g.	oben genannte(r,s)
OLG	Oberlandesgericht
OTT-Dienste	„Over-the-Top“-Dienste (breitbandige Internetdienste)
OVG	Oberverwaltungsgericht
OZG	Onlinezugangsgesetz

P

PassG	Passgesetz
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz)
PGP	Pretty Good Privacy (ein Standard zur Verschlüsselung)
PFS	Perfect Forward Secrecy
PNR	Passenger Name Records (Fluggastdaten)

Q

R

RÄStV	Rundfunkänderungsstaatsvertrag
Rdnr.	Randnummer
RED-G	Gesetz über die Einrichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus
RStV	Rundfunkstaatsvertrag

S

s.	siehe
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SGB	Sozialgesetzbuch
SIP	Session Initiation Protocol (Netzwerkprotokoll zum Aufbau und zur Steuerung einer Kommunikationssitzung)
SNK	Sicheres Netz der Kassenärztlichen Vereinigungen
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
sog.	sogenannte(r)
SpielbG LSA	Spielbankgesetz des Landes Sachsen-Anhalt
StatG-LSA	Landesstatistikgesetz Sachsen-Anhalt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

T

TCDP	Trusted Cloud Datenschutzprofil
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security (Sicherheitsprotokoll)
TMG	Telemediengesetz
TR	Technische Richtlinie (des BSI)
TTIP	Transatlantische Handels- und Investitionspartnerschaft

U

UIG	Umweltinformationsgesetz
UKlaG	Unterlassungsklagengesetz
USB	Universal Serial Bus (Universelles serielles Bussystem)
UWG	Gesetz gegen den unlauteren Wettbewerb
u. a.	unter anderem

V

VDA	Verband der Automobilindustrie
VEMAGS	Verfahrensmanagement für Großraum- und Schwertransporte
Verf LSA	Verfassung des Landes Sachsen-Anhalt
VG	Verwaltungsgericht
vgl.	vergleiche
VwVfG	Verwaltungsverfahrensgesetz

W

WLAN	Wireless Local Area Network

X

Y

Z

ZD	Zeitschrift für Datenschutz
ZDF	Zweites Deutsches Fernsehen
ZensVorbG 2011	Zensusvorbereitungsgesetz 2011
ZensVorbG 2021	Zensusvorbereitungsgesetz 2021
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZMB	Zentraler Meldebestand, Bezeichnung eines Fachverfahrens bei Dataport
ZMDB	Zentraler Meldedatenbestand
ZMDB-VO LSA	Verordnung zum Zentralen Meldedatenbestand des Landes Sachsen-Anhalt

1 Entwicklung und Situation des Datenschutzes

1.1 Neues Europäisches Datenschutzrecht

Die Berichtszeiträume waren von der Novellierung und grundsätzlichen Überarbeitung der datenschutzrechtlichen Grundlagen und Regelungen geprägt. Diese Prozesse begannen zuerst auf europäischer Ebene und setzten sich dann folgerichtig in der nationalen Gesetzgebung von Bund und Ländern fort.

Datenschutz und auch die Rechtsstellung seiner unabhängigen Aufsichtsbehörden sind europarechtlich zu verstehen. Das beeinflusst auch das Tätigwerden und Selbstverständnis des Landesbeauftragten für den Datenschutz in Sachsen-Anhalt. Datenschutz bzw. informationelle Selbstbestimmung gewinnt infolge der europäischen Maßgaben an Stärke und Durchsetzungskraft.

Die grundlegende Neugestaltung des Datenschutzrechts erfolgte durch das Inkrafttreten der „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“ (ABl. Nr. L 119 S. 1 vom 4. Mai 2016, ber. Nr. L 314 S. 72 vom 22. November 2016, ber. Nr. L 127 S. 2 vom 23. Mai 2018) am 25. Mai 2016. Die Kurzbezeichnung hierfür ist „Datenschutz-Grundverordnung“ (**DS-GVO**). Sie gilt nach einer Übergangszeit von 2 Jahren ab dem 25. Mai 2018 und findet unionsweit unmittelbare Anwendung.

Im Gegensatz zur DS-GVO musste die datenschutzrechtliche Vorgängerregelung, die „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (EG-Datenschutzrichtlinie), in nationales Recht umgesetzt werden. Dies führte dazu, dass das angestrebte einheitliche europäische Schutzniveau in der Praxis der einzelnen Mitgliedstaaten nicht zufriedenstellend erreicht wurde. Auch die technische und wirtschaftliche Weiterentwicklung seit 1995 machte eine Anpassung an die neuen datenschutzrechtlichen Anforderungen notwendig (zu Einzelheiten der DS-GVO s. Nr. 3.1.1).

Trotz der zweijährigen Übergangszeit zeigten sich Wirtschaft, Behörden, aber auch die Politik überrascht von den ab dem 25. Mai 2018 zu beachtenden neuen Datenschutzregelungen der DS-GVO. Der Landesbeauftragte hatte bereits seit 2016 im Rahmen seiner Möglichkeiten u. a. in besonderen Veranstaltungen – insbesondere mit Multiplikatoren wie den berufsständischen Vertretungen, Wirtschaftsverbandsvertretern, den Datenschutzbeauftragten der Landkreise, den kommunalen Spitzenverbänden etc. – über die Neuregelungen informiert.

Obwohl sich die grundsätzlichen datenschutzrechtlichen Vorgaben in vielen Bereichen inhaltlich nicht wesentlich verändert haben, werden die Regelungen oftmals zunächst als zusätzliche Belastung durch die verantwortlichen Stellen empfunden. Dem trat der Landesbeauftragte auch mit dem Argument entgegen, dass das neue Datenschutzrecht auch eine Chance ist. Verbraucherinnen und Verbraucher sind grundsätzlich eher bereit, ihre personenbezogenen Daten mit Unternehmen zu teilen, wenn sie diesen vertrauen können und hinsichtlich ihrer verarbeiteten Daten auch

konkrete Rechte geltend machen können. Wer konsequent auf hohe Datenschutzstandards setzt und diese seinen Kunden transparent mitteilt, hat klare Wettbewerbsvorteile. Sinngemäß gilt das auch für Behörden, wenn durch konsequenten Datenschutz das Vertrauen der Bürgerinnen und Bürger in die Verwaltung gestärkt wird.

Der Landesbeauftragte hat gemäß den europäischen Vorgaben sowohl Sensibilisierungs- und Beratungsaufgaben als auch Anordnungs- und Sanktionsbefugnisse. In dieser Reihenfolge und mit diesem Selbstverständnis werden die vielen Anfragen und Beschwerden bearbeitet. Schon nach dem Inkrafttreten der DS-GVO am 25. Mai 2016 und insbesondere in der Start- und Übergangsphase seit dem 25. Mai 2018 wirkte der Landesbeauftragte oftmals als Ratgeber zum Zwecke des Möglichmachens von Datenverarbeitungen unter gleichzeitiger Gewährleistung des Datenschutzes. Diese Rolle und Funktion wird weiterhin einen erheblichen Anteil in der alltäglichen Tätigkeit behalten.

Die DS-GVO gilt grundsätzlich unmittelbar in allen Mitgliedstaaten und bedarf nicht mehr einer Umsetzung im nationalen Recht. Gleichwohl enthält sie sowohl eingeräumte Regelungsoptionen („Öffnungsklauseln“) als auch konkrete Regelungsaufträge, die im nationalen Recht zu nutzen oder auszufüllen sind.

Aus diesem Grunde hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im Berichtszeitraum in verschiedenen Entschließungen sowohl zur DS-GVO und ihren Folgen Stellung genommen als auch eigene Vorschläge unterbreitet (vgl. **Anlagen 4, 5, 6, 18**).

Auf Bundesebene wurde mit Blick auf die DS-GVO mit dem „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2026/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097) ein neues Bundesdatenschutzgesetz (BDSG) erlassen (s. Nr. 3.1.3).

In Sachsen-Anhalt wurden zunächst mit dem „Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes“ vom 21. Februar 2018“ (GVBl. LSA S.10) und dem „Sechsten Medienrechtsänderungsgesetz“ vom 29. März 2018 (GVBl. LSA S. 22) zunächst die obligatorischen Öffnungsklauseln in Artikel 54 der DS-GVO (Errichtung der Aufsichtsbehörde) und Artikel 85 der DS-GVO (Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit) ausgefüllt. Der sich darüber hinaus im allgemeinen und im bereichsspezifischen Datenschutzrecht des Landes ergebende Regelungs- und Anpassungsbedarf soll mit einem „Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an das Recht der Europäischen Union“ (DSAnpG EU LSA) und durch weitere Anpassungen im Fachrecht aufgegriffen werden.

Neben der DS-GVO wurde auf europäischer Ebene die „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“ verabschiedet (ABl. Nr. L 119 S. 89). Diese Richtlinie, die rechtliche Regelungen und Vorgaben für die Bereiche

der Justiz und Polizei enthält, war nach einer Übergangszeit von zwei Jahren bis zum 6. Mai 2018 in nationales Recht umzusetzen. Sie wird auch als sog. „JI-Richtlinie“ (J für Justiz und I für Inneres) bezeichnet. Wegen der Einzelheiten wird auf Nr. 3.1.2 verwiesen.

Abgeschlossen werden soll die Reform des Europäischen Datenschutzrechts durch eine Überarbeitung der Verordnung (EG) Nr. 45/2001 (diese betrifft die Datenverarbeitung bei der EU und ihren Organen) sowie durch die Schaffung einer neuen Verordnung zum Datenschutz in der elektronischen Kommunikation (E-Privacy-Verordnung, s. Nr. 5.1).

1.2 Digitalisierte Gesellschaft

Parallel zum neuen Europäischen Recht und dessen Ausfüllung und Umsetzung auf nationaler Ebene schreitet auch die Digitalisierung der Gesellschaft weiter voran. Auch im Rückblick auf Grundsatzaussagen in vergangenen Tätigkeitsberichten lässt sich sagen:

Digitalisierung durchdringt alle Lebensbereiche und hält dabei vielfältige Chancen bereit. Selbstorganisation, Informationsgewinnung und Kommunikation ohne Computer und Smartphone sind für viele Menschen bereits unvorstellbar geworden. Digitale Agenden prägen alle Politikbereiche. Das Land Sachsen-Anhalt formulierte seine Ziele und Erwartungen an die neue, digitale Welt von morgen in einer eigenen Digitalen Agenda im Dezember 2017. Heilserwartungen an das Internet sind zwar enttäuscht worden; doch es entwickelt sich unaufhaltsam weiter. Neue Trends, Produkte, Möglichkeiten begegnen uns in immer kürzerer Folge und werfen immer neue Fragen auf. Wie kann Datenschutz z. B. mit der Unveränderlichkeit der Blockchain-Technologie kompatibel sein? Darf zur Meidung eines sozialen Netzwerks geraten werden, weil es sich nicht datenschutzgerecht betreiben lässt und obwohl es jedermann nutzt? Wird sich das Agieren der Internetkonzerne durch das Eingreifen von Wettbewerbs- und Kartellbehörden begrenzen lassen? Sind die Forderungen des technischen Datenschutzes aus der seit 25. Mai 2018 geltenden Datenschutz-Grundverordnung (DS-GVO) – Data Protection by Design and by Default – bei der Hardware-Produktion und in der Softwareentwicklung und -anwendung durchsetzbar? Sind Passwörter noch zeitgemäß? Darf der Staat zum Hacker werden?

Entwicklungen wie das Internet der Dinge, Big Data, Industrie 4.0 über Wirtschaft 4.0 bis zur Gesellschaft 4.0, künstliche Intelligenz, die digitale Vermessung des Menschen und seines Verhaltens (Profiling, Tracking) drängen informationelle Selbstbestimmung, Verhaltensfreiheit und Gedankenfreiheit weiter in die Defensive.

Vorhersagen dienen dazu, das Verhalten der Verbraucher und Internetnutzer zu beeinflussen. Zu Eingriffen in Freiheitsrechte kommen zusätzlich Diskriminierungen infolge algorithmischer Entscheidungen. Mensch oder Maschine – hat Privatsphäre eine Zukunft?

Viele Internetnutzer tragen zur Überwachungsgesellschaft bei. Ihr Verhalten ist jedoch widersprüchlich: Obwohl sie nicht überwacht werden wollen und etwa die Videoüberwachung des Nachbarn scharf angreifen und nach dem Staat als Beschützer rufen, geben sie doch stetig Daten von sich preis. Dass sie angeblich nichts zu verbergen haben und es „freiwillig“ tun, nutzt dem Staat und den neuen Geschäftsmo-

dellen der Wirtschaft. Ein neues Verständnis von „Datensouveränität“ betont den ökonomischen Wert von Daten.

Das Recht – und das schließt zumal die DS-GVO ein – tut sich bisweilen schwer mit den Big-Data-Anwendungen, etwa im Gesundheitsbereich. Jedenfalls läuft das Recht zumeist der Technik hinterher. Letztlich bleibt die Frage: Wie können künstliche Intelligenz und Big Data mit den Grundsätzen des Datenschutzes vereinbart werden? Das erfordert auch einen neuen Dialog zwischen Wirtschaft, Staat, Wissenschaft und Datenschutz.

Auch laufen die Informations- und die Datensicherheit häufig den technischen Entwicklungen hinterher. Datenunsicherheiten entstehen oft unbemerkt im Laufe der Zeit. Gefährdungen der sog. Cybersicherheit sind Alltag. Alten und neuen Gefahren, wie Denial-of-Service-Attacken (Überflutung von Servern mit Anfragen), DNS-Spoofing (Fälschung von Namensauflösungen), Zombie-Computern und Botnetzen, Ransomware (WannaCry) und omnipräsenten Hardware-Sicherheitslücken (Spectre, Meltdown) müsste konsequenter begegnet werden.

Das alles stellt Datenschützer vor gewaltige Herausforderungen. Die Aufgaben der Aufsichtsbehörden in der Europäischen Union wachsen; doch ihre Möglichkeiten wirksamer Kontrolle und Gestaltung sind u. a. abhängig von Haushaltsmitteln.

Greifen aber die bisherigen Prinzipien und Maßstäbe überhaupt bei den Entwicklungen der digitalen Gesellschaft? Ist die Frage „Mensch oder Maschine“ noch zulässig? Muss anstelle von Politik, Recht, Kontrolle und Technik – auch anstelle von Technikfolgenabschätzungen (auch des Gesetzgebers, der aber bei dieser Aufgabe seiner Verantwortung nicht gerecht wird) und Datenschutz durch Technik – nun vorrangig auf Ethik, Selbstkontrolle und Datenschutz durch Bildung (vgl. Nr. 9.2.4) und damit mehr Nutzerkompetenz gesetzt werden? Ist ein solcher Ansatz aber hinreichend wirksam? Sollte der mündige Konsument und Internetnutzer aufgeklärt und in die Pflicht genommen werden, selbst zu handeln, oder ist es nicht gerade Aufgabe staatlicher Fürsorgepflicht, den Konsumenten zu entlasten, und die Verursacher übermäßiger Datenverarbeitung in die Verantwortung zu nehmen?

Einige dieser Fragestellungen sollen auch durch zwei neue Gremien behandelt werden: Die Chancen der Digitalisierung soll der Digitalrat der Bundesregierung in den Blick nehmen. Mit möglichen Konflikten im Bereich der Datenpolitik soll sich eine neue Datenethikkommission befassen. Eine Enquete-Kommission des Bundestages befasst sich mit Auswirkungen künstlicher Intelligenz; die Bundesregierung will eine „Strategie Künstliche Intelligenz“ erarbeiten.

Ethik und Medienbildung wirken nicht hinreichend gegenüber machtvollen Internetkonzernen. Internetkonzerne wie Microsoft, Apple, Facebook oder Google müssen mit den Datenschutz-Aufsichtsbehörden in Europa konstruktiv zusammenarbeiten und entsprechende Lösungen finden, um Datenschutz in ihre Produkte zu integrieren. Der mündige Internetnutzer verlangt nach Produkten, die „ab Werk“ datenschutzgerecht eingestellt sind. Die nunmehr geltende DS-GVO hat viele Menschen sensibilisiert, dies zeigt sich nicht zuletzt in den aktuellen Anfragen und Beschwerden beim Landesbeauftragten.

Ethik und Medienbildung allein sind wirkungslos vor allem gegenüber dem Staat selbst. Dieser greift als Präventionsstaat im Kampf um Sicherheit sowie gegen Terrorismus und internationale Kriminalität immer mehr in Freiheitsräume des Bürgers ein (vgl. Nr. 1.3). Daten werden vorsorglich auf Vorrat gesammelt. Analysesysteme werten weit im Vorfeld von Gefahren und Straftaten auch Daten aus sozialen Netzwerken aus. Neue Datenpools vermischen die Zwecke der Datenverarbeitung. Der „demokratische Überwachungsstaat“ schwächt den Rechtsstaat in seinen Fundamenten. Kritik am Datenschutz führt bis zu dessen Diskreditierung.

Insgesamt geht es bei den Gefährdungen und Schädigungen des Persönlichkeitsrechts um den Freiheitsgedanken und darüber hinaus zusätzlich um das Demokratieprinzip. Dessen Bewährungsprobe hat schon begonnen. Das Gefühl des Überwachtwerdens macht den einzelnen Menschen zum Objekt. Das Verbot der Totalüberwachung und Totalregistrierung ist Teil der Verfassungsidentität. Die Überwachungslogik beschädigt das Vertrauen in die Stabilität des demokratischen Gemeinwesens. Das schwächt auch die E-Government-Angebote des Staates, die zwar in den Digitalen Agenden verankert sind, sich jedoch nicht auf Augenhöhe mit den Erwartungen des Bürgers und der Wirtschaft befinden.

Damit hängt schließlich noch ein ganz anderer Aspekt zusammen: Wie gelingt eine Teilhabe der in der analogen Welt Bleibenden? Wie wird das Recht auf informationelle Nichtbestimmung beachtet und umgesetzt?

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat vor dem Hintergrund dieser vorerwähnten Entwicklungen eine Reihe von Positionen in ihrer Göttinger Erklärung vom 30. März 2017 zusammengefasst (**Anlage 15**). Wesentlich bleiben folgende Aussagen: Die Menschenwürde ist zentraler Maßstab im digitalen Zeitalter. Datenschutz ist wertvoll. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

1.3 Sicherheit und Freiheit

In seinem XII. Tätigkeitsbericht (Nr. 1.1) hat der Landesbeauftragte dargestellt, wie durch Maßnahmen des Gesetzgebers bzw. deren Unterlassen die Freiheitsgrundrechte vernachlässigt werden und der Datenschutz immer öfter als Verhinderungsinstrument wirksamer Kriminalitäts- und Terrorismusbekämpfung und als vermeintlicher Täterschutz kritisiert wird. Dazu bleibt weiterhin nur festzustellen, wie es die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder anlässlich ihrer 91. Konferenz im Jahre 2016 formuliert hat: „Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen“ (**Anlage 3**).

Seine 18. Legislaturperiode (2013 bis 2017) hat der Deutsche Bundestag auch dazu genutzt, weitere Regelungen zu schaffen, die der Erhöhung der Sicherheit in der Bundesrepublik Deutschland dienen sollen. Fraglich bleibt aber, ob mehr Sicherheit allein durch mehr Sicherheitsgesetze erreicht werden kann. Die Auswirkungen auf die Freiheitsprinzipien der demokratischen Gesellschaft sind jedenfalls gravierend. Der angemessene Ausgleich zwischen Sicherheit und Freiheit ist nicht mehr gewahrt.

Eine Bedrohungslage durch die verschiedenen Formen des Extremismus und Terrorismus wird nicht verkannt. Der Zugewinn für die Sicherheit durch viele Maßnahmen des Gesetzgebers ist jedoch eher ungewiss. Gewiss ist aber, dass die Freiheit des Einzelnen – und dazu zählt auch die Freiheit der informationellen Selbstbestimmung – erheblich und in vielen Fällen rein vorsorglich schon im Vorfeld von Gefährdungslagen beeinträchtigt wird.

Wie die Erfahrungen der vergangenen Jahrzehnte zeigen, bedarf es offensichtlich immer wieder erst einer gerichtlichen Abwägung, um den Freiheitsrechten ihre angemessene Wirkungskraft zukommen zu lassen.

Ein Beispiel ist die Entscheidung des EuGH vom Dezember 2016 zur sog. Vorratsdatenspeicherung (s. Nr. 8.1). Das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ aus dem Jahr 2015 muss sich nun auch vor dem Bundesverfassungsgericht an dem messen lassen, was der EuGH sehr deutlich formuliert hat.

Die Wahrung der Freiheitsgrundrechte wäre die vordringliche Aufgabe, stattdessen arbeitet die Bundesregierung auf eine weitergehende Professionalisierung der Überwachungsmechanismen hin. Als Beispiel soll hier die Einrichtung von ZITiS dienen. ZITiS ist die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“. Sie hat ihren Sitz in München und versteht sich als Dienstleister für die Sicherheitsbehörden in Deutschland. Die Aufgaben orientieren sich nach dem Selbstbild am Bedarf der Sicherheitsbehörden und umfassen die Bereiche digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse wie auch technische Fragen der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr. ZITiS hat keine Eingriffsbefugnisse; ZITiS entwickelt und testet Strategien, technische Lösungen und Werkzeuge mit Cyberbezug und koordiniert gemeinsame Projekte für die deutschen Sicherheitsbehörden. ZITiS arbeitet im Ergebnis an technischen Möglichkeiten, in die Informations- und Kommunikationssysteme der Menschen mit Möglichkeiten des aktuellen Standes der Technik einzugreifen.

Auf der anderen Seite steht mit dem BSI, dem Bundesamt für die Sicherheit in der Informationstechnik, eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft zur Verfügung. Dieses hat die Aufgabe, Sicherheitslücken in der Informationstechnik bei Behörden und Unternehmen zu erkennen und diese zu bekämpfen. Das BSI versucht genau das zu verhindern, was ZITiS versucht zu befördern: Hintertüren finden oder ggf. schaffen und ausnutzen.

Ob dabei der Grundrechtsschutz ausreichend gewahrt wird, bleibt mehr als zweifelhaft. Die Regelung zum Staatstrojaner im BKA-Gesetz von 2017 steht ebenfalls auf dem Prüfstand des Bundesverfassungsgerichts. Die heimliche Installierung von Überwachungssoftware in Computer und Smartphones beschädigt das Vertrauen der Nutzer in eine freie Kommunikation und auch in staatlichen Schutz und dürfte mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nur schwerlich vereinbar sein.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die **Geschäftseingänge** entwickelten sich wie folgt:

2015: 5.230 2016: 5.506 2017: 6.737

Die Eingänge verteilten sich wie folgt:

Öffentliche Stellen:
2015: 3.823 2016: 3.673 2017: 4.546

Nichtöffentliche Stellen:
2015: 1.407 2016: 1.833 2017: 2.191

Zu den vorgenannten Zahlen kamen wiederum viele telefonische Behörden- und Firmenanfragen hinzu. Die Mitarbeiter und Mitarbeiterinnen der Geschäftsstelle des Landesbeauftragten nahmen zahlreiche Beratungsgespräche wahr. Infolge der DS-GVO kam es schon vor deren Anwendungsbeginn im Jahre 2018 zu weiteren Steigerungen (Geschäftseingänge erstes Quartal 2018: 2.044; zweites Quartal 2018: 6.769).

Kontrollen bei öffentlichen wie nichtöffentlichen Stellen erfolgten überwiegend anlassabhängig. Trotz der hohen Arbeitsbelastungen hielt der Landesbeauftragte auch in diesen Berichtszeiträumen daran fest, auch wieder anlassunabhängige Kontrollen durchzuführen. In Bezug auf öffentliche Stellen wurden wieder Schwerpunkte gesetzt (Kontrollen u. a. durch Querschnittsprüfungen in Kommunen, die Kontrolle eines großen Forschungsprojektes an den Universitäten des Landes, bei einer Krankenkasse in Bezug auf Krankengeld (individuelle Beratung und Hilfestellung), den Besuch von verschiedenen Schulen, einem Jobcenter und einem Personalamt).

Durch eigene Seminare und Beteiligung an einem Seminar haben sich Beschäftigte des Landesbeauftragten auch wieder an **Fortbildungen** für Behördenbedienstete beim Aus- und Fortbildungsinstitut des Landes beteiligt.

Weiter hielten der Landesbeauftragte und einzelne Mitarbeiter bei verschiedenen Behörden, Organisationen und Bildungseinrichtungen **Vorträge** zur Entwicklung des Datenschutzes, insbesondere zu neuen europarechtlichen Vorgaben sowie zu fachspezifischen Themen. Auch konnten auf Anregung des Landesbeauftragten im Zusammenwirken mit dem Ministerium für Inneres und Sport und den kommunalen Spitzenverbänden in zwei Veranstaltungen die Grundzüge der DS-GVO für die kommunalen Hauptverwaltungsbeamten dargestellt werden. Auch in weiteren Vorträgen im kommunalen Bereich bzw. für einzelne Ämter wurden teilweise dreistellige Zuhörerzahlen erreicht.

Im Bereich der Wirtschaft wurden in Zusammenarbeit mit Branchen- und anderen Unternehmensverbänden etliche **Informationsveranstaltungen** durchgeführt, wodurch eine Vielzahl von Unternehmen und deren Datenschutzbeauftragte erreicht werden konnten. Hervorzuheben ist die Zusammenarbeit mit den Industrie- und Handelskammern, den Handwerkskammern und den für die freien Berufe zuständi-

gen Kammern, die der Landesbeauftragte zunächst über das seit dem 25. Mai 2018 anzuwendende Datenschutzrecht informierte und die fortan als Multiplikatoren fungierten. Die Veranstaltungen werden nach dem 25. Mai 2018 fortgeführt; Schwerpunkte sind zunehmend Auslegungs- und Anwendungsfragen der DS-GVO und des BDSG 2018. Auch für Landesverbände von Vereinen fanden und finden Informationsveranstaltungen statt.

Auf der Homepage des Landesbeauftragten werden vielfältige Informationen zum neuen Datenschutzrecht (Kurzpapiere der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Vortragsfolien, Mustertexte und weitere Arbeitshilfen) vorgehalten (vgl. im Übrigen auch die Angaben der Landesregierung in LT-Drs. 7/3175). Der Landesbeauftragte entwickelt seine Service-Angebote stetig fort und berücksichtigt dabei auch die Abstimmungsergebnisse aus den Gremien der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Auch die Datenschutzkonferenz besitzt nunmehr eine eigene Homepage; das Informationsangebot umfasst u. a. deren Positionsbestimmungen und Links zum Datenschutzrecht des Bundes und der Länder.

Allen Organisatoren von Informationsveranstaltungen gilt der besondere Dank des Landesbeauftragten.

Wie bisher hat der Landesbeauftragte wieder regelmäßig den **Erfahrungsaustausch** mit den behördlichen Datenschutzbeauftragten der kreisfreien Städte und Landkreise durchgeführt und sich am Erfahrungsaustausch der behördlichen Datenschutzbeauftragten der Hochschulen des Landes beteiligt.

Auch der regelmäßige Austausch mit den Datenschutzaufsichtsbehörden des Bundes und der Länder wurde fortgesetzt. Dies ist u. a. deshalb notwendig, weil häufig auch die zu kontrollierenden Einrichtungen, wie beispielweise die Allgemeinen Ortskrankenkassen bundesweit vernetzt agieren und sich austauschen. Auch im Beschäftigtendatenschutz ist es notwendig, bundesweit agierenden Unternehmen abgestimmt gegenüberzutreten.

Im Zusammenhang mit den Herausforderungen der Europäischen Datenschutz-Grundverordnung hat sich der Arbeitsaufwand der Aufsichtsbehörden erheblich intensiviert (vgl. Nr. 2.3).

2.2 Schwerpunkte

Mit beträchtlichem Zeitaufwand verbunden war auch die Beratung der Landesregierung in Bezug auf Rechtssetzungsvorhaben.

Hervorzuheben sind insoweit die umfänglichen Beratungen mit dem Ministerium für Inneres und Sport im Hinblick auf die notwendigen gesetzgeberischen Reaktionen auf die Vorgaben der Europäischen Datenschutz-Grundverordnung und der Richtlinie EU 2016/680 (sog. „JI-Richtlinie“); s. Kapitel 3.1.

Weitere Beratungsgegenstände in der Gesetzgebung betrafen:

- E-Government-Gesetz (s. Nr. 4.4)

- Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) und Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums für polizeiliche Telekommunikationsüberwachung (s. Nrn. 6.2, 6.6)
- Änderung des Schulgesetzes (s. Nr. 9.2.2)
- Landeskrebsregistergesetz (s. Nr. 10.1.6)

Wichtige Einzelfälle und längerfristige Vorgänge betrafen:

- Dataport (s. Nr. 4.6)
- Elektronischer Rechtsverkehr in der Justiz (s. Nr. 8.2)
- Forschungsprojekt Nationale Kohorte (s. Nr. 9.1.1)
- Vermittlung von Medienkompetenz (s. Nr. 9.2.4)
- Digitalisierung im Schulbereich (s. Nrn. 9.2.5, 4.12)
- Zentrales Landesprojekt zur Förderung der Berufswahlkompetenz von Schülerinnen und Schülern (s. Nr. 9.2.7)
- Kontrolle der Webshops von Apotheken (s. Nr. 10.1.7)
- Prüfung in der Wohnungswirtschaft (s. Nr. 13.10)
- Videoüberwachung in Bäckereien (s. Nr. 14.1.8)

2.3 Organisationsfortentwicklung des Landesbeauftragten

Seit dem Jahre 1992 war die Geschäftsstelle des Landesbeauftragten für den Datenschutz beim Präsidenten des Landtages eingerichtet. Der Struktur nach wurde die Geschäftsstelle als Eingabe- und Petitionsstelle für den Bereich des öffentlichen Datenschutzes errichtet. Seit Herbst 2011 ist der Landesbeauftragte für den Datenschutz auch für den nichtöffentlichen Bereich (z. B. Wirtschaft, Vereine) als Aufsichtsbehörde zuständig. Darüber hinaus nimmt der Landesbeauftragte für den Datenschutz seit 2008 die Aufgaben des Landesbeauftragten für Informationsfreiheit wahr.

Der Landesbeauftragte für den Datenschutz und die Geschäftsstelle standen in den Berichtszeiträumen vor der größten Umstrukturierung ihrer Geschichte. Durch die neuen europäischen Grundlagen und nationalen Rahmenbedingungen wurde aus der Eingaben- und Petitionsstelle eine eigenständige, unabhängige Aufsichtsbehörde. Dieser wurden neue zusätzliche Aufgaben, Pflichten und Befugnisse – auch im nichtöffentlichen Bereich – übertragen.

Die Übertragung geschieht im Wesentlichen durch:

- Die EU-Datenschutz-Grundverordnung (DS-GVO). Sie gilt unmittelbar als Gesetz und ersetzt überwiegend die bestehen Datenschutzgesetze des Bundes und der Länder.

- Die sog. JI-Richtlinie[1]. Sie gibt verbindliche rechtliche Vorgaben für die deutschen Umsetzungsgesetze in den Bereichen Justiz und Inneres vor.
- Nationale Rechtsprechung und Gesetze (z. B. Antiterrordatei-, Rechtsextremismusdatei-, Unterlassungsklagengesetz).

Unabhängig von den erheblichen gesetzlichen Ausweitungen der Aufgaben und Befugnisse des Landesbeauftragten werden sich zusätzliche Arbeitsfelder sowohl durch die technischen als auch die gesellschaftlichen Entwicklungen ergeben. Neue Tätigkeitsfelder, die von der Aufsichtsbehörde zu bewältigen sind, kommen zwingend aus der weiteren Digitalisierung von Wirtschaft, Staat und Gesellschaft. Beispielhaft seien hier die Stichworte „Wirtschaft 4.0“, „E-Government“ (einschließlich Dataport) und die umfangreiche Vernetzung bis in den privaten Bereich („Smarte Welten“) genannt (s. Nr. 1.2).

Aufgrund der zwingenden gesetzlichen Vorgaben (Art. 52 DS-GVO: „völlige Unabhängigkeit“) war die Geschäftsstelle aus der Anbindung bei der Landtagspräsidentin und der Landtagsverwaltung herauszulösen. Dies hatte zur Folge, dass der Teil der Verwaltungsaufgaben, den die Landtagsverwaltung für den Landesbeauftragten wahrgenommen hat, nunmehr von der Behörde selbst übernommen werden musste. Insbesondere sind hier die Bereiche Personal und Haushalt, einschließlich der Funktion der Beauftragten für den Haushalt, zu nennen, die von der Behörde nunmehr selbst personell untersetzt werden müssen.

Ergänzend wird angemerkt, dass mit der Loslösung der Geschäftsstelle aus dem Landtagsbereich neben den Kerntätigkeiten nunmehr auch verschiedene Beauftragte zu stellen sind (z. B. Schwerbehindertenbeauftragter, Gleichstellungsbeauftragte, Korruptionsbeauftragter, Geheimschutzbeauftragter, Sicherheitsbeauftragter usw.). Auch ist ein eigener Personalrat erforderlich.

Aus der erheblichen Erweiterung der Aufgaben, Verpflichtungen und auch Befugnisse ergibt sich ein neuer, höherer Stellenbedarf. Auch aus diesem Grunde haben die Aufsichtsbehörden der Länder ein Gutachten zum „zusätzlichen Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung“ in Auftrag gegeben, dass von Herrn Prof. Dr. Alexander Roßnagel erstellt und im Januar 2017 vorgelegt wurde. In diesem Gutachten wird dargelegt, dass für die Umsetzung allein der Vorgaben aus der DS-GVO durchschnittlich zusätzliche 28 Stellen je Aufsichtsbehörde erforderlich wären. Nicht berücksichtigt von diesem Gutachten wurden die weiteren Personalbedarfe im Rahmen der Umsetzung der JI-Richtlinie, der neuen gesetzlichen Aufgaben durch nationales Recht und Rechtsprechung und der Übernahme von Verwaltungsaufgaben, die bislang von der Landtagsverwaltung bearbeitet worden sind (insbesondere Personal und Haushalt). Auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat zu den Ausstattungserfordernissen der neuen Behörden Stellung genommen (**Anlage 8**).

---

[1] 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 2008/1977/JI des Rates (ABl. Nr. L 119 S. 89)

Im Rahmen der Aufstellung des Entwurfs des Haushaltsplanes für die Haushaltsjahre 2017/2018 meldete der Landesbeauftragte den Bedarf von nur 16 weiteren Stellen für seine Geschäftsstelle an. Die der Anmeldung zugrundeliegenden Personalplanungen orientierten sich dabei am Grundsatz der sparsamen Haushaltsführung. Sie stellte eine Mindestausstattung dar. Inwieweit diese neue angestrebte Personalstruktur für die zukünftigen Bedarfe ausreichend gewesen wäre, sollte abgewartet werden, um dann in späteren Haushaltsaufstellungen bedarfs- und zielgerecht weitere Anmeldungen vornehmen zu können (insbesondere sollten weitere Personalbedarfe anhand der praktischen Erfahrungen mit der europäischen Regelung, Vorgaben und Verfahrensweisen aber auch anhand der konkreten Bedarfe von Bürgern, Unternehmen, Vereinen und Behörden für die Folgehaushalte evaluiert werden).

Trotz ausführlicher Begründung der weiteren Personalbedarfe und der Vorlage des Gutachtens wurden dem Landesbeauftragten vom Parlament auf Vorschlag des Finanzausschusses lediglich pauschal nur 4 Stellen bewilligt. Damit wurde die gesetzliche Garantie, dass dem Landesbeauftragten für den Datenschutz die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen ist (§ 21 Abs. 3 Satz 2 DSG LSA), nicht erfüllt.

Anfang 2018 verabschiedete der Landtag das Gesetz zur Organisationsentwicklung des Landesbeauftragten für den Datenschutz (GVBl. LSA S. 10). Mit diesem am 6. Mai 2018 in Kraft getretenen Gesetz wurden verschiedene Regelungen des geltenden Datenschutzgesetzes Sachsen-Anhalt (DSG LSA) neu gefasst und ein Teil der Vorgaben, die aus der DS-GVO und der JI-Richtlinie folgten, umgesetzt. Gemäß der Neufassung des § 21 Abs. 3 DSG-LSA wurde die Geschäftsstelle beim Landesbeauftragten für den Datenschutz selbst eingerichtet. Damit waren die Verwaltungsaufgaben, die bislang die Landtagsverwaltung wahrgenommen hatte, nunmehr in eigener Verantwortlichkeit zu bewältigen.

Trotz der Übertragung dieser neuen Verwaltungsaufgaben und der gesetzlichen Garantie aus § 21 Abs. 3 Satz 2 DSG LSA wurden vom Landtag nicht die erforderlichen Stellen zur Aufgabenbewältigung bewilligt. Es wurde lediglich die Berechtigung eingeräumt, Aufgaben der Personalverwaltung auf eine andere Stelle des Landes zu übertragen, wenn diese zustimmt. Die Unabhängigkeit des Landesbeauftragten darf hierdurch aber nicht beeinträchtigt werden (§ 21 Abs. 3 Satz 6 DSG LSA). Nach Inkrafttreten dieser Regelung hat der Landesbeauftragte sämtliche Ministerien, den Landesrechnungshof und die Landtagsverwaltung angefragt, ob die Übernahme der Personalverwaltung möglich sei. Keine Behörde sah sich in der Lage, die mit der Übernahme der Personalverwaltung verbundenen zusätzlichen Aufgaben zu übernehmen. Aus den Ablehnungen der Anfrage wird deutlich, wie stark die Belastung allein durch die Übernahme der Personalverwaltung ist, wenn selbst große Institutionen wie Ministerien sich nicht in der Lage sehen, die Personalverwaltung des Landesbeauftragten zu übernehmen. Noch nicht berücksichtigt sind die zusätzlichen Arbeitsbelastungen, die mit der Übernahme von Haushaltsangelegenheiten verbunden sind.

Vor diesem Hintergrund wurden für die Aufstellung des Einzelplanes 2019 erneut auf das bereits 2016 vorgelegte Personalkonzept für eine Mindestausstattung der Geschäftsstelle zurückgegriffen und die fehlenden 12 Stellen erneut angemeldet. Der Landesbeauftragte erwartet, dass im Sinne seiner völligen Unabhängigkeit die aus seiner Sicht erforderliche Personalausstattung von der Landesregierung dem Land-

tag im Rahmen des Haushaltsentwurfs ungeschmälert vorgelegt wird. Eine Einflussnahme der Landesregierung wäre europarechtswidrig. Der Landesbeauftragte ist hier in einer vergleichbaren Position wie der Landesrechnungshof.

2.4 Sichere Kommunikation mit dem Landesbeauftragten

Bereits am 16. September 2015 wurde der PGP-Schlüssel des Landesbeauftragten für den Datenschutz Sachsen-Anhalt ausgetauscht. Der alte Schlüssel ist weiterhin lesbar, wird aber nicht mehr verwendet. Der neue Schlüssel des Landesbeauftragten wurde vom Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, als Betreiber der gemeinsamen CA der Datenschutzbehörden des Bundes und der Länder, beglaubigt. Der Fingerabdruck des neuen Schlüssels für die primäre Benutzerkennung „LfD Sachsen-Anhalt <poststelle@lfd.sachsen-anhalt.de>" lautet „5CBB 4E15 9774 8921 3B27 7C96 DE25 9BE2 09AC A0DE“ und läuft am 14. September 2020 ab.

Das aktuelle X.509-Zertifikat der Landes-PKI des Landesbeauftragten hat den Fingerabdruck: „1F B0 7E AC FC E9 E0 4F 1A 40 17 A7 F4 D4 B0 6C 11 76 4C BC“ (SHA1) und ist bis zum 12. November 2019 gültig.

Des Weiteren kann ein Zertifikat der D-Trust GmbH genutzt werden, welches für den Bürger (mit modernem E-Mail-Client und Betriebssystem) einfacher installierbar sein sollte. Es hat den Fingerabdruck „F2 C6 69 48 46 05 38 4C A6 18 3E 7F 94 0A 0C F3 A4 C1 5B EF“ (SHA1) und ist bis zum 29. April 2019 gültig.

Leider erfordert die Installation immer noch sehr viel Handarbeit. Bis heute ist es nicht gelungen, einen Standard zu etablieren, der die Zertifikatssuche komplett automatisiert. Bei PGP könnten doppelte Schlüssel gefunden werden, bei X.509 muss zumindest das Zertifikat selbst zur Prüfung vorliegen und auch dann ist offen, ob die passenden Wurzel-Zertifikate automatisiert gefunden werden können. Aber eigentlich sollte ein moderner E-Mail-Client einfach anhand der E-Mail-Adresse das Zertifikat anfordern und komplett prüfen können! Hier rächt es sich, dass bei der Einführung des neuen Personalausweises (nPA) nicht von Anfang an einfach nutzbare kryptografische Schlüssel an alle Bürger (und Behörden) kostenfrei ausgegeben und etablierte Standards ignoriert wurden. Stattdessen wurden vergleichsweise teure Portale und Anwendungen für De-Mail, das Elektronische Gerichts- und Verwaltungspostfach und aktuell für das besondere Behördenpostfach aufgebaut, die zwar funktionieren, aber alles in allem nur die Identifikation und Verteilung der Schlüssel nachträglich vornehmen und die Nutzung solcher „sicheren“ Dienste unnötig verteuern und erschweren. Richtiges E-Government geht anders.

Der Landesbeauftragte schlägt vor, dass sich die Landesregierung dafür einsetzt, dass z. B. mit Hilfe des bereits existierenden nPA dem Bürger überprüfbare Softzertifikate für die alltägliche Nutzung z. B. im E-Mail-Client zur Verfügung gestellt werden. Diese sollen nicht primär der digitalen Unterschrift, sondern der Verbesserung der IT-Sicherheit allgemein dienen. Frei nutzbare Internet-Dienste könnten die jeweils gültigen, öffentlichen Zertifikate verteilen und auf Anfrage prüfen, Plugins in den E-Mail-Clients könnten sich um die sichere, transparente und einfache Nutzung der Infrastruktur kümmern. Das wäre eine

Möglichkeit, die eigene eID zu nutzen und so dem Bürger eine einfache Verschlüsselung normaler E-Mails zu ermöglichen.

Für die Meldung des Datenschutzbeauftragten gem. Art. 37 Abs. 7 DS-GVO, die Meldung einer Datenpanne gem. Art. 33 DS-GVO und für Anfragen oder Beschwerden gem. Art. 77 DS-GVO wurden auf der Homepage des Landesbeauftragten einfach und sicher nutzbare Formulare eingerichtet. Eingaben werden dabei zwischen Webbrowser und Web-Server https-verschlüsselt übertragen. Dort erfolgen eine Verschlüsselung mit GnuPG und der Weitertransport via E-Mail.

3 Nationales und internationales Datenschutzrecht

3.1 Neue Rechtsgrundlagen

3.1.1 Datenschutz-Grundverordnung

Bereits im XI. und XII. Tätigkeitsbericht (jeweils Nr. 3.1.1) berichtete der Landesbeauftragte über die seinerzeit noch nicht verabschiedete Europäische Datenschutz-Grundverordnung (DS-GVO). Mittlerweile haben sich der Europäische Rat, das Europäische Parlament und die Europäische Kommission über deren Inhalt geeinigt. Die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ wurde am 27. April 2016 verabschiedet (ABl. L 119/1). Sie ist seit dem 25. Mai 2018 unmittelbar anzuwenden.

Die DS-GVO hat insbesondere Bedeutung für die Wirtschaft und andere Verantwortliche im nichtöffentlichen Bereich, z. B. Vereine. Auch private Haushalte müssen sich bei der Verarbeitung personenbezogener Daten an die DS-GVO halten, sofern es nicht um die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten geht.

Aber auch im behördlichen Bereich ist die DS-GVO grundsätzlich anzuwenden. Sie gilt lediglich nicht in Bereichen,

- die vom europäischen Recht ausgenommen sind (z. B. Nachrichtendienste),
- die der Außen- und Sicherheitspolitik unterfallen und
- die unter die sog. JI-Richtlinie fallen (siehe Nr. 3.1.2).

Für den Bereich der Bereitstellung öffentlicher elektronischer Kommunikationsdienste in öffentlichen Netzen siehe Nr. 5.1.

Die DS-GVO stellt für alle Verantwortlichen eine Herausforderung dar. Ihre Einhaltung ist schon deshalb erforderlich, weil es um die Grundrechte von betroffenen Personen geht (Kunden, Beschäftigte, Geschäftspartner, Bürger). Diese haben nunmehr vielfältige Rechtsschutzmöglichkeiten: Sie können Beschwerde bei der Aufsichtsbehörde einreichen oder direkt im Zivilrechtsweg gegen den Verantwortlichen klagen (einschließlich Geltendmachung von Schadensersatzansprüchen). Dabei können sie sich z. B. durch Verbraucherverbände oder ähnliche Organisationen vertreten las-

sen. Sog. anspruchsberechtigte Stellen haben ein eigenes Verbandsklagerecht gegen bestimmte Datenschutzverstöße (vgl. XII. Tätigkeitsbericht, Nr. 1.2).

Daneben kann der Landesbeauftragte nach wie vor die Verarbeitung von personenbezogenen Daten beschränken oder verbieten. Nach der DS-GVO besteht diese Befugnis erstmals auch gegenüber Behörden. Zudem ist der Bußgeldrahmen für nichtöffentliche Stellen drastisch erhöht worden. Konnten nach § 43 Abs. 2 des bisher geltenden BDSG Bußgelder in Höhe bis zu lediglich 300.000 Euro festgesetzt werden, liegt die Obergrenze nach der DS-GVO bei 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens.

Auf die seinerzeit zu erwartenden wesentlichen Neuerungen hat der Landesbeauftragte bereits im XII. Tätigkeitsbericht (Nr. 3.1.1) hingewiesen. Bei diesen Neuerungen ist es geblieben. Dazu ist insbesondere auf Folgendes aufmerksam zu machen:

- Es bleibt beim sog. Verbot mit Erlaubnisvorbehalt. Das heißt, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn eine wirksame Einwilligung vorliegt oder eine Rechtsvorschrift dies gestattet.

- Neu ist das Recht auf Datenübertragbarkeit. Danach müssen die von der betroffenen Person bereitgestellten Daten – soweit technisch machbar – an sie oder einen anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden, wenn die Verarbeitung automatisiert erfolgt und auf einer Einwilligung oder einem Vertrag beruht.

- Neu ist ebenfalls das Recht auf Vergessenwerden. Hat der Verantwortliche zu löschende Daten zuvor öffentlich bekannt gemacht, muss er angemessene Maßnahmen treffen, um die Verantwortlichen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person die Löschung verlangt hat.

- Deutlich erweitert wurden die Informationspflichten der Verantwortlichen. Über den Werbewiderspruch hinaus besteht zudem ein Widerspruchsrecht in weiteren besonderen Situationen, welches dazu führen kann, dass keine Weiterverarbeitung zulässig ist.

- Umfangreicher gestaltet wurden Dokumentations- und Nachweispflichten. So muss der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten ebenso wie die Einwilligung nachweisen.

- Für alle Verarbeitungen muss ein Verzeichnis von Verarbeitungstätigkeiten geführt werden. Ausnahmen gelten nur in bestimmten Fällen für kleine Unternehmen.

- Eine Datenschutz-Folgenabschätzung muss immer durchgeführt werden, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat. Kann der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos treffen, ist die Aufsichtsbehörde zu konsultieren.

- Im Falle der Verletzung des Schutzes personenbezogener Daten (sog. Datenpannen) muss der Verantwortliche möglichst binnen 72 Stunden diese der Aufsichtsbehörde melden.

- Bei der Einrichtung von Systemen und Diensten muss von Anfang an der Datenschutz durch Technikgestaltung (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) gewährleistet werden.

- Technische Systeme müssen unter Berücksichtigung des aktuellen Stands der Technik in der Lage sein, Belastungen standzuhalten (bereits zuvor hatten u. a. Diensteanbieter nach § 13 Abs. 7 TMG durch technische und organisatorische Vorkehrungen sicherzustellen, dass technische Einrichtungen gegen Verletzungen des Schutzes personenbezogener Daten gesichert sind).

Zwar ist die DS-GVO als verbindliches europäisches Recht (eine Verordnung wirkt wie ein Gesetz) durch die Verantwortlichen unmittelbar anzuwenden. Sie enthält jedoch etliche Regelungsaufträge und Regelungsoptionen zugunsten der Mitgliedstaaten der Europäischen Union. Daher wird es eine Fülle von nationalen Vorschriften geben, die ergänzend zu beachten sind; zumal für öffentliche Stellen. Für den Bereich des allgemeinen Datenschutzes wurde bereits ein neues Bundesdatenschutzgesetz verabschiedet (BGBl. I 2017, S. 2097 ff.), s. dazu Nr. 3.1.3.

Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass sie die Vorgaben der DS-GVO und ggf. des BDSG 2018 umgesetzt haben. Dabei ist besonders wichtig, von der Verarbeitung personenbezogener Daten betroffene Prozesse und Strukturen sowie die Datenschutzorganisation zu überprüfen. Einzelfragen sind dabei, ob ein Datenschutzbeauftragter bestellt werden musste, die Rechtsgrundlagen für die Verarbeitung geklärt worden sind, die Informationspflichten und Betroffenenrechte erfüllt werden und ob sichergestellt wurde, dass Verarbeitungen im erforderlichen Maß dokumentiert werden und gewährleistet ist, dass im Falle von Datenpannen schnell reagiert werden kann (vgl. auch zum Datenschutzmanagement nichtöffentlicher Stellen unter Nr. 13.2).

Vielfältige Informationen hierzu stellt der Landesbeauftragte auf seiner Homepage zur Verfügung. Beachtenswert sind insbesondere die Hinweise der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK-Kurzpapiere).

3.1.2 JI-Richtlinie

Neben der DS-GVO wurde auf europäischer Ebene am 27. April 2016 auch die „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates 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“ verabschiedet (ABl. Nr. L 119 S. 89). Sie trat am 5. Mai 2016 in Kraft.

Diese sog. JI-Richtlinie gilt aber nicht automatisch und unmittelbar. Vielmehr ist sie, um Geltung zu erlangen, in nationales Recht umzusetzen. Aus diesen Grunde gibt die Richtlinie in Art. 63 Abs. 1 vor, dass die Mitgliedstaaten bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften erlassen, die erforderlich sind, um der Richtlinie nachzukommen. Die Mitgliedstaaten hätten die Vorschriften seit dem 6. Mai 2018 anwenden müssen.

Ziel der JI-Richtlinie ist es, für den Datenschutz in den Bereichen Polizei und Justiz eine Mindestharmonisierung innerhalb der Union zu gewährleisten und insgesamt ein höheres Datenschutzniveau in der EU zu erreichen. In Deutschland waren bzw. sind eine Vielzahl von Bundes- und Landesgesetzen entsprechend den Vorgaben der JI-Richtlinie zu novellieren.

Der Bundesgesetzgeber hat mit dem „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2026/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 ein neues Bundesdatenschutzgesetz (BDSG) erlassen (BGBl. I S. 2097). Dieses Gesetz trat am 25. Mai 2018 in Kraft. Spezielle Regelungen für den Bereich Justiz und Polizei enthält das neue BDSG („BDSG 2018“) in seinem dritten Teil.

In Sachsen-Anhalt wurde zunächst mit dem „Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes“ vom 21. Februar 2018 (GVBl. LSA, S.10) eine erste Teilumsetzung realisiert. Der Landesbeauftragte für den Datenschutz wurde gem. § 21 Abs. 1 Nr. 2 DSG LSA als Aufsichtsbehörde im Sinne von Art. 3 Nr. 15 in Verbindung mit Art. 41 der JI-Richtlinie errichtet. Gleichzeitig wurden mit § 22 Abs. 1 Satz 4 DSG LSA die Aufgaben und Befugnisse i. S. d. Art. 46 und 47 der Richtlinie übertragen.

Zur weiteren Umsetzung der JI-Richtlinie hat die Landesregierung im Juli 2018 den „Entwurf des Gesetzes 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“ dem Landtag vorgelegt (LT-Drs. 7/3207).

Mit dem vorgelegten Artikelgesetz soll ein einheitliches Querschnittsdatenschutzrecht für Polizei und Justiz angestrebt werden. Dieses soll mit dem “Gesetz zur Umsetzung der Richtlinie (EU 2016/680“ (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt – DSUG LSA) erreicht werden. Das DSG LSA ist nicht mehr maßgeblich. Daneben sollen bereichsspezifische Regelungen im Gesetz über die öffentliche Sicherheit- und Ordnung des Landes Sachsen-Anhalt (SOG LSA) sowie im Maßregelvollzugsgesetz an die Vorgaben der JI-Richtlinie angepasst werden.

Die Abgrenzung der Tätigkeiten der Behörden im Hinblick auf die Anwendung von JI-Richtlinie und DS-GVO erfolgt aufgabenbezogen, nicht behördenbezogen. Straftatenverhütung und -verfolgung, jegliche Gefahrenabwehr im Zusammenhang mit diesen Zwecken, dazu Strafvollstreckung und Verfolgung von Ordnungswidrigkeiten unterfallen dem Anwendungsbereich der Richtlinie. Wenn es sich um Gefahrenabwehr allein zum Zwecke der Gewährleistung der öffentlichen Ordnung handelt, greift die DS-GVO unmittelbar.

Der Landesbeauftragte war im Vorfeld der Erstellung des o. a. Artikelgesetzes u. a. im Rahmen des „Interministeriellen Arbeitskreises (IMA) Datenschutz“ eingebunden. Jedoch wurden seine Anregungen und Kritikpunkte, insbesondere hinsichtlich des SOG LSA, nur teilweise berücksichtigt (s. LT-Drs. 7/3207). Aus diesem Grunde ist beabsichtigt, in den Beratungen des Landtages datenschutzrechtliche Verbesserungen vorzuschlagen.

Für den Bereich des Justizvollzuges (insbesondere Untersuchungshaft, Strafhaft, Jugendstrafhaft, Sicherungsverwahrung und Jugendarrest) hat das Ministerium der Justiz trotz des Fristablaufes der Umsetzungsvorgabe am 6. Mai 2018 keinen Gesetzentwurf vorgelegt. Dieser Regelungsbereich war aus dem Entwurf des o. a. Artikelgesetzes ausgeklammert worden, da eine vom Strafvollzugsausschuss der Länder eingesetzte Arbeitsgruppe einen Mustergesetzentwurf erarbeiten sollte. Angesichts der zweijährigen Übergangszeit und des Ablaufs des Umsetzungstermins im Mai 2018 ist eine zeitnahe europarechtskonforme Umsetzung der Richtlinie im Justizvollzug dringend geboten.

3.1.3 Das neue Bundesdatenschutzgesetz

Am 5. Juli 2017 wurde das „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)“ im Bundesgesetzblatt veröffentlicht (BGBl. I 2017, S. 2097). Dieses Gesetz ist wie die DS-GVO seit dem 25. Mai 2018 anzuwenden. Wesentlicher Bestandteil des Gesetzes ist der Artikel 1, der das neue Bundesdatenschutzgesetz (**BDSG 2018**) enthält. Damit trat das bisherige Bundesdatenschutzgesetz (BDSG) ebenfalls am 25. Mai 2018 außer Kraft.

Mit dem DSAnpUG-EU sollen die nationalen Regelungen an die DS-GVO angepasst und insbesondere die zahlreichen Regelungsoptionen genutzt und Regelungsaufträge erfüllt werden. Es ist daher für die Verantwortlichen in vielen Fällen erforderlich, DS-GVO und BDSG 2018 zu beachten. Daneben wird es noch eine Fülle von bereichsspezifischen Datenschutzvorschriften geben, die den allgemeinen datenschutzrechtlichen Regelungen des BDSG 2018 vorgehen und die derzeit auf Bundesebene (vgl. BT-Drs. 19/3341) und Landesebene erarbeitet werden.

Das BDSG 2018 enthält besondere Vorschriften für nichtöffentliche Stellen, für öffentliche Stellen des Bundes und für öffentliche Stellen der Länder. Letzteres jedoch nur, wenn keine landesrechtlichen Regelungen bestehen. Für die Landesbehörden Sachsen-Anhalts wird diese Maßgabe keine Wirkung entfalten, da das Ministerium für Inneres und Sport beabsichtigt, für Sachsen-Anhalt an einem eigenen Datenschutzgesetz festzuhalten (s. Nr. 3.1.4). Darüber hinaus gilt das BDSG 2018 für öffentliche Stellen des Bundes, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind.

Eine wesentliche Regelung für die Aufsichtsbehörden betrifft die Festlegung der Vertretung im Europäischen Datenschutzausschuss (EDSA) und der zentralen Anlaufstelle. Dass diese Aufgabe nach § 17 BDSG 2018 die oder der Bundesbeauftragte für den Datenschutz wahrnehmen soll, leuchtet nicht unmittelbar ein, da die oder der Bundesbeauftragte im nichtöffentlichen Bereich lediglich für die Kontrolle von Post- und Telekommunikationsunternehmen zuständig ist. Sinnvoll wäre es gewesen, die

Vertretung und die Anlaufstelle einem von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder gewählten Mitglied zu übertragen.

Bedeutsam ist das Antragsrecht der Aufsichtsbehörden auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission (§ 21 BDSG 2018). Diese Regelung ist überfällig, da sie bereits aufgrund der EG-Datenschutz-Richtlinie von 1995 (RL 95/46 EG) erforderlich war und in der sog. Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015 (C-362/14, Rz 65) angemahnt wurde. Auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat in ihrer Entschließung vom 20. April 2016 dieses Recht gefordert (**Anlage 7**).

Nicht akzeptabel ist die Regelung des § 29 Abs. 3 BDSG 2018, wonach die Aufsichtsbehörden keine Kontrollbefugnisse bei Berufsgeheimnisträgern haben, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten führen würde. Damit ist keine wirksame Datenschutzkontrolle bei Ärzten, Rechtsanwälten und anderen in § 203 des Strafgesetzbuches benannten Berufsgruppen möglich. Nach Ansicht des Landesbeauftragten verstößt diese Regelung gegen die DS-GVO. Hier wurden die Grenzen einer Regelungsoption überschritten. Zwar können die Mitgliedstaaten nach Art. 90 Abs. 1 DS-GVO Kontrollbefugnisse der Aufsichtsbehörden regeln. Allerdings kommen nur Regelungen in Betracht, die notwendig und verhältnismäßig sind, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Eine mitgliedstaatliche Regelung darf nicht dazu führen, dass die Verarbeitung personenbezogener Daten, die dem Berufsgeheimnis unterliegen, in Gänze nicht kontrolliert werden kann.

Die §§ 32-37 BDSG 2018 erhielten die Überschrift „Rechte der betroffenen Person“. Die Überschrift erweckt allerdings einen falschen Eindruck, werden doch in diesem Kapitel hauptsächlich die in der DS-GVO manifestierten Rechte erheblich eingeschränkt. Die Verantwortlichen und die Aufsichtsbehörden haben hier die Aufgabe, die im BDSG 2018 enthaltenen Einschränkungen europarechtskonform auszulegen.

Zu begrüßen ist die Aufrechterhaltung der Regelung zur Benennung eines Datenschutzbeauftragten. Dieser ist nach § 38 Abs. 1 BDSG 2018 zu bestellen, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Stets ist ein Datenschutzbeauftragter zu bestellen, wenn eine Datenschutz-Folgenabschätzung erforderlich ist oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt und Meinungsforschung verarbeitet werden.

Das BDSG 2018 enthält zahlreiche Regelungen insbesondere für den nichtöffentlichen Bereich. Für die Wirtschaft wird die Herausforderung darin bestehen, die Regelungen des BDSG 2018 neben die der DS-GVO zu legen und die richtigen Schlüsse zu ziehen, insbesondere bei den Betroffenenrechten. Fraglich erscheint, ob bei allen Detailregelungen die Grenzen von Regelungsoptionen eingehalten wurden. Es bleibt abzuwarten, ob einzelne Bestimmungen – z. B. die über die eingeschränkten Kontrollbefugnisse der Aufsichtsbehörden bei Berufsgeheimnisträgern – noch geändert werden.

3.1.4 DSG LSA

Nach den Vorgaben der DS-GVO war das Landesdatenschutzrecht bis zum 25. Mai 2018 anzupassen. Hierzu hat sich die Landesregierung für ein stufenweises Vorgehen entschieden. Zunächst wurde in einem ersten Schritt im Gesetz zur Fortentwicklung der Organisation des Landesbeauftragten die Ausgestaltung der Aufsichtsbehörde in völliger Unabhängigkeit (s. Art. 51 ff. DS-GVO) geregelt, die schon in der Vorbereitung vorheriger DSG-Novellen erörtert wurde (siehe dazu XII. Tätigkeitsbericht, Nr. 3.1.3). Ein wichtiger Aspekt war dabei zunächst die Verselbständigung der Geschäftsstelle, die nicht mehr bei der Präsidentin des Landtags angebunden ist. Der Landesbeauftragte wurde ab dem Haushaltsjahr 2018 aus dem Einzelplan des Landtages herausgelöst und erhielt einen eigenen Einzelplan.

In diesem Zusammenhang ist der Präsidentin und den bisherigen Präsidenten des Landtages und ihren Mitarbeiterinnen und Mitarbeitern in besonderem Maß für die langjährige, umfängliche und freundliche Unterstützung insbesondere in den Bereichen der Haushalts- und Personalverwaltung zu danken.

Das Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt vom 21. Februar 2018 trat am 6. Mai 2018 in Kraft (GVBl. LSA, S. 10), s. zu Einzelheiten Nr. 2.3. Eine wesentliche Regelung der Änderung des Datenschutzgesetzes betrifft die Institutionalisierung des Landesbeauftragten als Aufsichtsbehörde nach europäischem Recht (§ 21 Abs. 1 Satz 1 DSG LSA).

In einem zweiten Schritt ist die Richtlinie (EU) 2016/680 in Landesrecht umzusetzen (vgl. ausführlich Nr. 3.1.2). Dies betrifft im Wesentlichen die Bereiche von Polizei und Staatsanwaltschaften, soweit sie der Strafverfolgung dienen, und allgemein die Verfolgung von Ordnungswidrigkeiten. Der Gesetzentwurf umfasst u. a. den Entwurf eines Gesetzes zur Umsetzung dieser Richtlinie (**DSUG LSA**) und die Änderung des SOG LSA. Der Landesbeauftragte wurde vom Ministerium für Inneres und Sport beteiligt. Der Gesetzentwurf liegt dem Landtag zur Beratung vor (LT-Drs. 7/3207).

Ein dritter Schritt soll im Rahmen der Anpassung des Datenschutzrechts an die europäischen Vorgaben mit dem Entwurf eines Gesetzes zur Ausfüllung der DS-GVO und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (**DSAG LSA**) erfolgen. Es soll Bestandteil eines Artikelgesetzes sein (Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an das Recht der Europäischen Union), in dem auch andere Gesetze angepasst werden sollen (u. a. Informationszugangsgesetz, Archivgesetz, Statistikgesetz). Das DSAG LSA soll das DSG LSA materiellrechtlich ersetzen und wird voraussichtlich erst Anfang 2019 in Kraft treten können. Bis dahin ist nach dem bisherigen DSG LSA, allerdings unter Beachtung der höherrangigen DS-GVO, zu verfahren. Da im Organisationsfortentwicklungsgesetz noch nicht aufgenommen, betrifft eine wesentliche Regelung auch eine Änderung in der Landeshaushaltsordnung: Es geht dabei um eine von Einflussnahmen unabhängige Geltendmachung von Haushaltsanmeldungen durch den Landesbeauftragten gegenüber dem den Haushalt aufstellenden Ministerium und gegenüber dem Landtag.

Ebenso sind im Fachrecht des Landes weitere Anpassungen vorgesehen. Im Bereich des Medien-, des Presse- und des Schulrechts sind sie auf den Weg gebracht. Im Übrigen arbeiten die Ressorts an den Anpassungen und stimmen sich in dem Inter-

ministeriellen Arbeitskreis Datenschutz, an dem sich der Landesbeauftragte beteiligt, ab.

Um die Gegenstände, die Geltungsbereiche und deren Abgrenzung gemäß den o. a. Gesetzen zu erläutern, empfahl der Landesbeauftragte, eine Handreichung bzw. einen Leitfaden für die öffentlichen Stellen des Landes herauszugeben, was jedoch im Berichtszeitraum nicht gelang. Das Ministerium für Inneres und Sport sollte dies unverzüglich nachholen.

3.1.5 Beschäftigtendatenschutz

Die Forderung nach einer sachdienlichen und differenzierten gesetzlichen Gestaltung des Beschäftigtendatenschutzes ist schon sehr alt (siehe XI. und XII. Tätigkeitsbericht, Nr. 3.1.2); leider ist es noch nicht zu einer umfassenden Schaffung eines Beschäftigtendatenschutzgesetzes gekommen (vgl. die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6. und 7. April 2016, **Anlage 4**).

Die Möglichkeiten hierzu sind auch für die Zukunft durch den Handlungsspielraum von Art. 88 DS-GVO gegeben. Danach können Mitgliedstaaten Rechtsvorschriften oder Kollektivvereinbarungen erlassen, um den Schutz von Rechten und Freiheiten hinsichtlich der Verarbeitung von personenbezogenen Beschäftigtendaten zu gewährleisten. Maßgeblich sind die Grundsätze der Datenverarbeitung nach der DS-GVO. Nach Art. 5 ist auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise zu verarbeiten.

Für den öffentlichen Bereich ist im Land Sachsen-Anhalt bisher eine grundlegende Ausgestaltung durch die Regelungen in § 50 BeamtStG, §§ 84 ff. LBG LSA gegeben. Insoweit bedarf es für die Tarifbeschäftigten einer Anpassung an die Vorgaben der DS-GVO mittels einer Fortführung der Regelung aus § 28 Abs. 1 DSG LSA. Dies ist im Entwurf eines DSAG LSA (s. Nr. 3.1.4) vorgesehen.

Für den nichtöffentlichen Bereich hat der Bundesgesetzgeber § 26 BDSG 2018 geschaffen (BGBl. I 2017, S. 2097, 2108), der am 25. Mai 2018 in Kraft trat. Die Regelung beschränkt sich inhaltlich im Wesentlichen auf die Aussagen in der bisherigen Regelung des § 32 BDSG. Beibehalten wird insbesondere eine Bestimmung, wonach die Vorgaben der Vorschrift auch gelten, wenn personenbezogene Daten nicht automatisiert oder in einem Dateisystem verarbeitet werden bzw. werden sollen (einzelne Papiervorgänge). Wie bisher ist die Datenverarbeitung zur Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses grundsätzlich zulässig. Neu ist die Regelung zur Verarbeitung besonderer Kategorien von personenbezogenen Daten (s. Art. 9 DS-GVO) in Absatz 3, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen überwiegt; zu den nach Art. 88 Abs. 2 DS-GVO vorgesehenen angemessenen und besonderen Maßnahmen zur Wahrung der menschlichen Würde und der Grundrechte der Betroffenen verweist die Regelung u. a. auf § 22 Abs. 2 BDSG 2018. Hinsichtlich der Einwilligung wird in § 26 Abs. 2 BDSG 2018 der Aspekt der Freiwilligkeit betont und die Schriftlichkeit gefordert.

Der Bedarf eines umfassenden und ausgewogenen Beschäftigtendatenschutzgesetzes besteht weiter.

3.2 Weitere europäische und internationale Entwicklungen

3.2.1 Privacy Shield

Im XII. Tätigkeitsbericht (Nr. 3.2.1) wies der Landesbeauftragte darauf hin, dass eine Übermittlung personenbezogener Daten in die USA auf Grundlage der sog. Safe-Harbor-Entscheidung der Europäischen Kommission vom 26. Juli 2000 nicht mehr zulässig ist und die Europäische Kommission mit den USA über ein neues Abkommen verhandelt. Seit dem 1. August 2016 enthält das EU-U.S. Privacy Shield Aussagen über den Schutz personenbezogener Daten, die aus einem Mitgliedstaat der Europäischen Union in die USA übertragen werden. Die Europäische Kommission hatte mit Beschluss vom 12. Juli 2016 entschieden, dass das Privacy Shield ein angemessenes Schutzniveau gewährleistet. Die Safe-Harbor-Entscheidung wird durch diesen Beschluss ersetzt. Ähnlich wie das Safe-Harbor-Abkommen kann das Privacy Shield den Datentransfer in die USA aber nur dann legitimieren, wenn ein Unternehmen nach dessen Regelungen zertifiziert ist.

Kritiker halten das Privacy Shield für nicht ausreichend. Die vorgesehenen Verfahren zum Schutz der Rechte von EU-Bürgern in den USA seien kompliziert und lückenhaft. Das Abkommen genüge damit nicht den vom EuGH aufgestellten Anforderungen (vgl. XII. Tätigkeitsbericht, Nr. 3.2.1). Die Artikel-29-Gruppe – der Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten – hielt das Privacy Shield gegenüber der alten Safe-Harbor-Regelung zwar für eine Verbesserung. Sie hatte jedoch auch erhebliche Bedenken, die sowohl von der Europäischen Kommission als auch von den US-Behörden ausgeräumt werden müssen. Insbesondere sollten der Ernennung einer unabhängigen Ombudsperson und von Mitgliedern des US-Aufsichtsgremiums für Datenschutz und Bürgerrechte Priorität eingeräumt werden. Die Einhaltung des Privacy Shield in den USA sollte durch das US-Handelsministerium stärker kontrolliert werden. Außerdem sollte es eine engere Zusammenarbeit zwischen den für den Datenschutz verantwortlichen Behörden in den USA und in der EU geben. Innerhalb der EU müssten potentiell Betroffene besser über die Rechte aufgrund des Privacy Shield und über die Beschwerdeverfahren informiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder teilte die Analyse der Artikel-29-Gruppe. Die kritische inhaltliche Bewertung hat sich der Europäische Datenschutzausschuss – als Nachfolgegremium unter der DS-GVO – zu eigen gemacht. Auch das EU-Parlament hat Nachbesserungen gefordert. Das Privacy Shield steht spätestens im Herbst 2018 auf dem Prüfstand.

Alternative Garantien zum Schutz des Persönlichkeitsrechts bei Übermittlung personenbezogener Daten in die USA bestanden in der Verwendung sog. Standardvertragsklauseln, verbindlicher Unternehmensregelungen oder Einzelverträgen (§ 4c Abs. 2 BDSG). Der oberste irische Gerichtshof hat dem EuGH am 3. Oktober 2017 die Frage vorgelegt, ob die EU-Standardverträge eine ausreichende Garantie zum Schutz der Privatsphäre bei Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWRs darstellen. Bis zu einer Entscheidung des EuGH können

Unternehmen weiterhin auf der Grundlage von Standardvertragsklauseln personenbezogene Daten in die USA übermitteln. Sollte der EuGH die Standardvertragsklauseln als nicht ausreichend beurteilen, sind Auswirkungen einer solchen Entscheidung auch auf verbindliche Unternehmensregelungen und auf die Privacy Shield-Entscheidung der Europäischen Kommission naheliegend.

Unternehmen, die personenbezogene Daten in die USA übermitteln, sollten die zu erwartende Entscheidung des EuGH beachten. Die DS-GVO sieht für Datentransfers in Länder außerhalb der EU/des EWRs folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- *Feststellung der Angemessenheit des Datenschutzniveaus im Empfängerland durch die EU-Kommission (Art. 45 DS-GVO),*
- *Vorliegen von in Art. 46 Abs. 2 und 3 DS-GVO genannten Garantien oder*
- *Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO).*

3.2.2 Fluggastdaten

Am 6. Juni 2017 wurde das Fluggastdatengesetz (FlugDaG) veröffentlicht (BGBl. I S. 1484), welches der Umsetzung der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. L 119 vom 4. Mai 2016, S. 132) dient. Im FlugDaG wird ein Datensatz von 20 verschiedenen Datenkategorien festgeschrieben, welcher bei jedem Flug an die Fluggastdatenzentralstelle zu melden ist. Diese Fluggastdatenzentrale ist im Bundeskriminalamt angesiedelt. Die Speicherung, die weitere Übermittlung und der Datenaustausch mit den Mitgliedsländern sowie die jeweilige Löschung der Daten unterliegen damit der Kontrolle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Eine Löschung der Daten aus dem Fluggastdaten-Informationssystem ist nach Ablauf von fünf Jahren vorgeschrieben. Jedoch sind Daten, die Angaben zur rassischen oder ethnischen Herkunft, zu politischen Meinungen, weltanschaulichen Überzeugungen, zur Mitgliedschaft in einer Gewerkschaft, zum Gesundheitszustand, zum Sexualleben oder zur sexuellen Orientierung einer Person beinhalten, unverzüglich, d. h. gleich nach Eingang der Daten, von der Fluggastdatenzentralstelle zu löschen.

Bereits im XII. Tätigkeitsbericht (Nr. 3.2.3) und auch in den Tätigkeitsberichten davor kritisierte der Landesbeauftragte die extrem lange Speicherdauer des sehr umfangreichen Datensatzes (Passenger Name Records – PNR-Daten), den die Fluggesellschaften für die jeweilige Beförderung erheben und der bereits vor Abflug an die jeweiligen Sicherheitsbehörden durch entsprechende Abkommen auch an Drittstaaten übermittelt werden sollen. Diese Abkommen sind verstärkt nach den Entwicklungen in der Welt, vor allem der Attentate und Terroranschläge, z. B. in Paris und Madrid, geplant worden bzw. zustande gekommen.

Zum geplanten Abkommen der Europäischen Union mit Kanada hat der EuGH am 26. Juli 2017 ein Gutachten (1/15) veröffentlicht, in welchem er dieses als teilweise unvereinbar mit den Bestimmungen europäischer Verträge und Grundrechte bewer-

tet. In diesem Gutachten wurden Grundsätze aufgestellt, unter welchen ein solches Abkommen europarechtlich zulässig wäre. An diesen Grundsätzen muss sich nunmehr auch die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 und damit auch das Fluggastdatengesetz messen lassen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verabschiedete hierzu in ihrer Sitzung am 9. November 2017 eine Entschließung unter dem Titel „Keine anlasslose Vorratsspeicherung von Reisedaten“ (**Anlage 17**).

3.2.3 Transatlantische Freihandelsabkommen

Im XII. Tätigkeitsbericht (Nr. 3.2.5) erläuterte der Landesbeauftragte die Bestrebungen der US-Regierung zur Schaffung einer Freihandelszone mit der EU, die sog. Transatlantische Handels- und Investitionspartnerschaft (TTIP). Dabei war nach Medienberichten davon auszugehen, dass die USA im Rahmen der Verhandlungen auf eine Absenkung des derzeitigen Datenschutzstandards hinwirken.

Derzeit scheinen die Verhandlungen mit den USA auf Grund der geänderten Politik der neuen amerikanischen Administration auf Eis zu liegen.

Gleichzeitig liegt das Freihandelsabkommen mit Kanada, das Comprehensive Economic and Trade Agreement (CETA), bereits vor. Zu diesem Abkommen hat der Ratifizierungsprozess bereits begonnen.

Die EU-Kommission hat Ende Januar 2018 beschlossen, dass künftig der Schutz personenbezogener Daten in Freihandelsabkommen nicht näher behandelt werden soll. Denn hierbei handele es sich in der EU um ein Grundrecht, welches nicht Verhandlungsgegenstand bei EU-Freihandelsabkommen sein kann.

3.2.4 Internationale Datenschutzkonferenzen

Im Gesamtberichtszeitraum fanden zwei Internationale Konferenzen der Beauftragten für den Datenschutz und die Privatsphäre statt.

Die 38. Internationale Datenschutzkonferenz in Marrakesch vom 17. bis 20. Oktober 2016 befasste sich u. a. mit den Herausforderungen, die die Entwicklung neuer Techniken für den Datenschutz mit sich bringt. Weiterhin wurden Entschließungen zu Kompetenzinhalten der Datenschutzerziehung, der Vereinheitlichung neuer Messgrößen zur Datenschutzregulierung und zur Förderung der internationalen Zusammenarbeit der Aufsichtsbehörden gefasst.

Im Rahmen der 39. Internationalen Datenschutzkonferenz in Hongkong vom 25. bis 29. September 2017 wurde u. a. über die Zusammenarbeit zwischen den Datenschutzbehörden und den Verbraucherschutzbehörden für einen besseren Schutz der Verbraucherinnen und Verbraucher in der digitalen Wirtschaft diskutiert und eine Resolution zum Datenschutz in automatisierten und vernetzten Fahrzeugen verabschiedet.

Wichtige Texte der Internationalen Konferenzen sind auf der Homepage des Landesbeauftragten unter dem Menüpunkt Konferenzen / Internationale Datenschutzkonferenz veröffentlicht.

3.2.5 Europäische Datenschutzkonferenzen

Vom 26. bis 27. Mai 2016 fand die Europäische Datenschutzkonferenz in Budapest statt. Hier wurden hauptsächlich die Umsetzung der DS-GVO auf europäischer und nationaler Ebene sowie das Verhältnis der DS-GVO zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) vom 28. Januar 1981 thematisiert.

Bei der darauffolgenden Europäischen Datenschutzkonferenz vom 27. bis 28. April 2017 in Limassol wurde eine Entschließung zur Modernisierung der Konvention 108 gefasst, wobei darauf verwiesen wurde, dass dies bereits in der Frühjahrskonferenz 2011 in Brüssel thematisiert worden war.

4 Technik und Organisation

4.1 Das Standard-Datenschutzmodell – SDM

Welche technischen und organisatorischen Maßnahmen sind erforderlich, um die datenschutzrechtlichen Anforderungen, insbesondere der seit 25. Mai 2018 geltenden Datenschutz-Grundverordnung (DS-GVO), zu erfüllen? Das betrifft insbesondere die Regelungen der Art. 5, 24, 25 und 32 der DS-GVO. Diese Frage stellen sich viele Behörden, Unternehmen und sonstige verantwortliche Stellen – aber auch die Datenschutzaufsichtsbehörden selbst, die diesen Stellen gegenüber eine Beratungs- und Kontrollfunktion ausüben.

Mit dem Standard-Datenschutzmodell (SDM) wurde federführend durch den Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) das Modell einer einheitlichen Prüfmethode entwickelt und etabliert, die es ermöglicht, die Frage systematisch und nachvollziehbar zu beantworten. Das SDM zeigt damit einen praktikablen Weg auf, rechtliche Vorgaben der DS-GVO in angemessene technische und organisatorische Maßnahmen umzusetzen. Grundlage dieses Modells bilden elementare Schutzziele, die sog. Gewährleistungsziele.

Hierzu gehören zum einen die klassischen Schutzziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Diese werden ergänzt um die speziell datenschutzbezogenen Anforderungen Datenminimierung, Transparenz, Intervenierbarkeit und Nichtverkettung. Das Gewährleistungsziel „Nichtverkettung“ bezeichnet die Anforderung, dass personenbezogene Daten nur für den Zweck verarbeitet und ausgewertet werden dürfen, für den sie erhoben wurden. Das SDM bezieht sich dabei nicht nur auf „Daten“. Als Verfahrenskomponenten werden Daten(bestände), IT-Systeme und Prozesse betrachtet. Ähnlich wie das bekannte IT-Grundschutz-Modell des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterscheidet auch das SDM drei Schutzbedarfe (normal, hoch, sehr hoch). Im Unterschied zum IT-Grundschutz-Modell des BSI wird dabei aber nicht das Unternehmen oder die Organisation betrachtet, sondern die einzunehmende Schutzperspektive des Betroffenen.

Das Konzept des SDM sieht vor, die Gewährleistungsziele heranzuziehen, um in methodischer Anlehnung an das IT-Grundschutz-Modell des BSI (aktuell: IT-Grundschutz-Kompendium – Edition 2018) die Schutzbedarfsfeststellungen hinsicht-

lich der Verarbeitung personenbezogener Daten zu ergänzen. Datenschutzanforderungen sind zum Teil sehr viel höher als Anforderungen an die IT-Sicherheit bzw. Informationssicherheit, wie sie u. a. vom IT-Grundschutz des BSI oder von Normen der ISO gefordert werden. Im Unterschied zum BSI-Grundschutz ist die Schutzperspektive aus der Sicht des Betroffenen formuliert und der Schutzbedarf aus der Eingriffsintensität bei der Verarbeitung personenbezogener Daten eines Verfahrens abgeleitet.

Aus der Analyse des Schutzbedarfs folgt dann, welche standardisierten Schutzmaßnahmen erforderlich sind. Die insoweit als erforderlich erkannten technischen oder organisatorischen Sicherungsmaßnahmen sollen zukünftig einem standardisierten Maßnahmenkatalog entnommen werden können, der als Anhang zum SDM konzipiert ist. In einer abschließenden Risikoanalyse können eventuell noch darüber hinaus gehende Sicherungsbedarfe ermittelt werden.

Die 92. DSK hatte im November 2016 eine erste Version des SDM verabschiedet. Nunmehr liegt mit einer Erprobungsfassung Version 1.1, die von der 95. DSK im April 2018 beschlossen wurde, eine aktualisierte Fassung vor. Diese ist auf der Homepage des Landesbeauftragten abrufbar.

Der Katalog mit den konkreten, standardisierten Schutzmaßnahmen wird von einer Unterarbeitsgruppe des Arbeitskreises Technik entwickelt, seine Veröffentlichung steht noch aus. Das SDM soll sowohl in der Kontroll- und Beratungspraxis der Datenschutzaufsichtsbehörden als auch bei der Planung, dem Betrieb und der permanenten Überwachung personenbezogener Datenverarbeitungsverfahren durch verantwortliche Stellen im öffentlichen und nichtöffentlichen Bereich erprobt werden. Es soll vom Arbeitskreis Technik laufend fortentwickelt werden.

Das SDM will verantwortliche Stellen im öffentlichen wie im nichtöffentlichen Bereich in die Lage versetzen, aus rechtlichen Anforderungen systematisch die erforderlichen technischen und organisatorischen Schutzmaßnahmen abzuleiten. Das SDM soll auch zu einer einheitlichen und transparenten Prüfpraxis der Datenschutzaufsichtsbehörden beitragen. Gelingt dies, dürfte das Modell vor dem Hintergrund der DS-GVO auch im europäischen Rahmen Beachtung und Anwendung finden.

4.2 Das neue Landesnetz – ITN-XT – rückt in weite Ferne

Für das Vorhaben der Landesregierung zur Schaffung eines hochmodernen Sprach- und Datennetzes für die Landesverwaltung (ITN-XT), als einem der zentralen Projekte der IKT-Strategie „Sachsen-Anhalt digital 2020“ vom 10. Oktober 2012 (MBl. LSA S. 585), wurden die Zuschläge durch das zuständige Ministerium der Finanzen des Landes Sachsen-Anhalt (MF) nach einer langwierigen europaweiten Ausschreibung und dem sich daran anschließenden Teilnehmerwettbewerb erteilt. Den Zuschlag für das ITN-XT (LOS 1: Aufbau, Migration und Betrieb eines Wide Area Networks (WAN) und mehrerer Local Area Networks in Standorten des Auftraggebers) und für die IP-Telefonie (LOS 2: Konzeption, Aufbau und Betrieb einer zentralen und georedundanten Voice-over-IP-Lösung (VoIP-Telefonie/SIP-Trunk) für die Landesverwaltung) erhielt die T-Systems International GmbH.

Bei der im LOS 2 für die VoIP-Telefonie vorgesehenen Lösung mittels SIP-Trunk (deutsch: Bündelung, Strang) handelt es sich um eine Technik, mit der Telefonanlagen über das SIP-Protokoll (Session Initiation Protocol) viele gleichzeitige, IP-basierte Sprachverbindungen über das Internet für ihre Nebenstellen mit einem Provider aufbauen können. Bei einem SIP-Trunk weist der Provider der TK-Anlage ganze Rufnummernblöcke und damit eine definierte Kapazität an gleichzeitig aufbaubaren Sprachkanälen zu.

Mit Hinweis auf die Geheimhaltungsvorschriften des europäischen Vergaberechts bezüglich des Vergabeverfahrens und der Auftragsvergabe wurden die Leistungsbeschreibungen dieser europaweiten Ausschreibung für das ITN-XT (LOS 1 und 2) und damit belastbare Informationen zu diesem Vorhaben von der damaligen Projektleitung auch gegenüber dem Landesbeauftragten verweigert. Der Landesbeauftragte hatte nach Rücksprache mit der Projektleitung des MF und nach Hinterlegung entsprechender Verschwiegenheitserklärungen zumindest Einsicht in diese Leistungsbeschreibungen erhalten. Er hat in diesen Zusammenhang Angaben in den Leistungsbeschreibungen hinterfragt und hierzu Hinweise gegeben. Nur diese Form der Beteiligung war möglich, da dem Landesbeauftragten aus den genannten Gründen keine Leistungsbeschreibungen überlassen werden konnten.

Grundsätzlich sind aus datenschutzrechtlicher und technischer Sicht die in den Leistungsbeschreibungen vorgesehenen Sicherheitsmaßnahmen positiv zu beurteilen. Hierzu gehören für den geplanten leistungsfähigen 40 GBit-Backbone des ITN-XT zwei redundant aufgebaute Technikstandorte, redundante Backbone-Systemkomponenten, redundante zentrale Firewalls nach CC-EAL-4 sowie redundante BSI-zertifizierte Layer-2-Verschlüsselungskomponenten bis zum Standort. Für besonders sicherheitsrelevante Bereiche ist eine zusätzliche Verschlüsselung über Layer-3 mittels IPSec vorgesehen.

Zudem ist für das gesamte ITN-XT bisher eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz geplant. Voraussetzung für die Vergabe eines solchen Zertifikats ist eine Überprüfung durch einen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten ISO 27001-Grundschutz-Auditor. An diesem Vorhaben hält das MF bislang noch fest.

Im Jahr 2017 wurden bereits ca. 100 Standortbegehungen zur Vorbereitung der Migration der Standorte vom derzeitigen ITN-LSA auf das ITN-XT durchgeführt. Das umfangreiche Vorhaben umfasst insgesamt den Anschluss von ca. 740 Verwaltungsstandorten an die WAN-Infrastruktur des ITN-XT sowie die Einrichtung des Zugangs von 137 Kommunen und 993 Schulen (Schulverwaltungsnetz).

Die Inbetriebnahme des Landesnetzes ITN-XT, so ist zu befürchten, verzögert sich weiter. Bereits im aktualisierten Umsetzungsplan vom März 2014 zur IKT-Strategie wurde die Inbetriebnahme des ITN-XT auf Ende 2017 korrigiert. Durch das MF wurde gegenüber allen Ressorts und auch dem Landesbeauftragten eine transparentere Informationspolitik angekündigt. Jedoch gibt es aktuell keinen konkreten Zeitplan zur Realisierung des ITN-XT.

Im Juni 2018 wurden in der Sitzung des IKT-Kreises durch die neue Projektleitung die wenig erfreulichen Ergebnisse der bisherigen Standortbegehungen vorgestellt:

Demnach ist unter Zugrundelegung der Anforderungen einer BSI-Grundschutzzertifizierung keiner der Standorte anschlussfähig.

Im Hinblick auf die ambitionierten Ziele der Digitalen Agenda des Landes Sachsen-Anhalt, die anstehende Einführung des Elektronischen Rechtsverkehrs und die Umsetzung der Anforderungen aus dem Onlinezugangsgesetz drängt nunmehr die Zeit, denn das ITN-XT bildet die eigentliche, sichere Infrastruktur für alle diese Vorhaben.

4.3 Informationssicherheitsleitlinie – noch immer nicht verabschiedet

Wie im Bund, so muss auch im Land eine „Cyber-Sicherheitsstrategie“ entwickelt werden. Mit Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie; ABl. L 194 vom 19. Juli 2016, S. 1) durch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 vom 23. Juni 2017 (BGBl. I S. 1885) und einer Änderung der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958) hat der Bund hierfür die gesetzlichen Voraussetzungen geschaffen.

In seinem XII. Tätigkeitsbericht (Nr. 4.2) hatte der Landesbeauftragte über die Verzögerung bei der Erarbeitung einer Landesleitlinie Informationssicherheit, deren Ausarbeitung im Zusammenhang mit der Umsetzung des aktualisierten Maßnahmenplans (Stand: 20. Mai 2014) der IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“ vom 10. Oktober 2012 (MBl. LSA S. 585) vorgesehen war, berichtet. Der IT-Planungsrat von Bund und Ländern (s. Nr. 4.5) selbst hatte bereits im März 2013 seine Leitlinie Informationssicherheit einschließlich des Umsetzungsplans beschlossen, die für alle Behörden des Bundes und der Länder Geltung besitzen und deren Vorgaben auch in einer Landesleitlinie Berücksichtigung finden sollten. Diese wiederum bildet eine wesentliche Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) mit Strukturvorgaben für die Landesverwaltung.

Die Landesregierung hatte in ihrer Stellungnahme zum XII. Tätigkeitsbericht des Landesbeauftragten vom 19. Januar 2017 (LT-Drs. 7/934) den Feststellungen des Landesbeauftragten, dass es spätestens mit der Ausarbeitung des E-Government-Gesetzes für das Land Sachsen-Anhalt einer Landesleitlinie zur Informationssicherheit bedarf, zugestimmt. Bis 2018 sollten alle wesentlichen Vorbereitungen zum In-Kraft-Treten einer solchen Landesleitlinie abgeschlossen sein und danach mit der Einführung eines ISMS für die gesamte Landesverwaltung begonnen werden. Die Zusammenarbeit in der Landes-Arbeitsgruppe InfoSic (Informationssicherheit) unter Beteiligung des Landesbeauftragten wurde dazu fortgesetzt.

Der im Umsetzungsplan zur IKT-Strategie geplante Termin, bis zum Jahr 2018 eine solche Leitlinie für Informationssicherheit zu verabschieden, ist nunmehr wieder in Gefahr. Die Arbeiten an der „Informationssicherheitsleitlinie“ wurden durch diese Arbeitsgruppe unter Federführung des Ministeriums der Finanzen (MF) erst im November 2016 wiederaufgenommen. Der Landesbeauftragte war daran beteiligt und hat in diesem Zusammenhang auf die Berücksichtigung und Beachtung der seit dem 25. Mai 2018 unmittelbar geltenden Datenschutz-Grundverordnung (DS-GVO) auf-

merksam gemacht. Die spezifischen Anforderungen der DS-GVO (Verordnung (EU) 2016/679) und der JI-Richtlinie (Richtlinie (EU) 2016/680) zur Sicherheit der Verarbeitung personenbezogener Daten müssen ihren Rückhalt auch in dieser Informationssicherheitsleitlinie finden. Die Anforderungen zur Datensicherheit müssen neben denen der Informationssicherheit berücksichtigt werden. Die Informationssicherheit schafft zum Teil erst die Voraussetzung für einen wirkungsvollen Datenschutz. Das ist in dem vorliegenden Entwurf einer „Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt – Informationssicherheitsleitlinie (Stand 01/2018) noch nicht der Fall.

Das MF beabsichtigt gleichwohl, mit einer Kabinettvorlage im Herbst 2018 die Voraussetzungen für ein landesweites ISMS zu schaffen. Angesichts des laufenden Gesetzgebungsverfahrens zu einem E-Government-Gesetz des Landes (s. Nr. 4.4) und der Anforderungen aus dem Onlinezugangsgesetz ist zu hoffen, dass dieser Zeitplan eingehalten wird und bei der Formulierung der Informationssicherheitsleitlinie die Anforderungen der DS-GVO Berücksichtigung finden.

4.4 E-Government-Gesetz Sachsen-Anhalt

Der Landesbeauftragte hat die Bemühungen der Landesregierung zur Schaffung eines modernen und zukunftsfähigen E-Government-Gesetzes von Beginn an begleitet. Spätestens mit dem am 1. August 2013 in Kraft getretenen Gesetz zur Förderung der elektronischen Verwaltung des Bundes (E-Government-Gesetz – EGovG) vom 25. Juli 2013 (BGBl. I S. 2749), mit dem die Bundesverwaltung grundlegend modernisiert wird, bestand auch für das Land Handlungsbedarf. Das Landesrecht hinkt gegenwärtig der Lebenswirklichkeit weit hinterher. Die Landesverwaltung ist, wenn sie Landesrecht ausführt, nicht verpflichtet, mit den Bürgerinnen und Bürgern auf deren Wunsch elektronisch zu kommunizieren. Auch die Kommunikation innerhalb der Verwaltung muss bisher nicht elektronisch erfolgen. Die elektronische Durchführung von Verwaltungsverfahren findet so gut wie nicht statt. Die Verwaltung arbeitet statt mit der elektronischen Akte weitgehend noch mit Papier. Die Menschen erwarten aber, dass sie mit der Verwaltung jederzeit ortsunabhängig in Kontakt treten und Verwaltungsvorgänge erledigen können. Und weil die Verwaltungsleistungen regelmäßig nicht von den Landesbehörden, sondern zum überwiegenden Teil von den Kommunen erbracht werden, müssen die Kommunen bei gesetzlichen Regelungen zum E-Government verbindlich und verpflichtend mit einbezogen werden.

Der Landesbeauftragte hatte daher gegenüber der Enquete-Kommission des Landtags „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“ die Einführung eines Landes-E-Government-Gesetzes mit den vorgenannten Inhalten angeregt. Die Enquete-Kommission des Landtags von Sachsen-Anhalt folgte in ihrem Abschlussbericht nach dreijähriger Tätigkeit am 1. September 2015 (LT-Drs. 6/4331 vom 31. August 2015) fraktionsübergreifend den damaligen Kernempfehlungen des Landesbeauftragten zum Schwerpunkt „E-Government-Strategie“. Gleichwohl waren seitens der Landesregierung Aktivitäten für eine ganzheitliche, nachhaltige, verbindliche, vernetzte und den Datenschutz und die Datensicherheit einbeziehende und umsetzende E-Government-Strategie und eine zügige Erarbeitung eines E-Government-Gesetzes für das Land Sachsen-Anhalt nicht zu erkennen. Dies hatte der Landesbeauftragte in seinem XII. Tätigkeitsbericht (Nr. 4.3) dementsprechend kritisiert.

Diese kritische Bestandsaufnahme des Landesbeauftragten zum schleppenden Fortgang der Erarbeitung eines E-Government-Gesetzes für das Land Sachsen-Anhalt wurde von der Landesregierung in ihrer Stellungnahme zum XII. Tätigkeitsbericht des Landesbeauftragten vom 19. Januar 2017 (LT-Drs. 7/934) nicht geteilt. Sie wies auf das am 28. Oktober 2015 in Kraft getretene Gesetz über die Organisation der Landesverwaltung Sachsen-Anhalt (Organisationsgesetz Sachsen-Anhalt – OrgG LSA) vom 27. Oktober 2015 (GVBl. LSA S. 554) und die in § 3 getroffenen Regelungen zur „Elektronischen Verwaltung“ hin. Sie legte ferner dar, dass im Koalitionsvertrag vom 19. April 2016 die Schaffung eines E-Government-Gesetzes vereinbart sei und die gemeinsamen Empfehlungen der Enquete-Kommission weitgehend berücksichtigt werden sollten. Die Landesregierung erklärte sogar ausdrücklich: „Der Empfehlung des Landesbeauftragten, die kommunale Ebene im vollen Umfang einzubeziehen, wird entsprochen“ (LT-Drs. 7/934, S. 18). Diesen Ankündigungen entsprachen sowohl die Referentenentwürfe als auch der dem Landtag zur Beratung vorgelegte Gesetzentwurf nicht.

Der Landesbeauftragte wurde frühzeitig in die Gesetzgebungsüberlegungen des zuständigen Ministeriums für Inneres und Sport (MI) einbezogen. Auf grundsätzliche Probleme machte er in seinen Stellungnahmen zu den Referentenentwürfen vom 15. Februar 2016, 30. August 2016 und vom 9. Dezember 2016 aufmerksam. Das betraf insbesondere die komplizierte Verweisungstechnik auf das EGovG des Bundes statt einer eigenen Vollregelung für das Land, die Differenzierung zwischen unmittelbarer Landesverwaltung und mittelbarer Landesverwaltung (insbesondere den Kommunen) sowie Regelungen, die nur für die unmittelbare Landesverwaltung und nicht für die Kommunen gelten sollten.

Bund und Länder hatten sich im Rahmen der Verhandlungen über eine Neuordnung der Bund-Länder-Finanzbeziehungen im 1. Halbjahr 2017 auch über eine Grundgesetzänderung im Bereich der Informationstechnik verständigt. Durch das Gesetz zur Änderung des Grundgesetzes vom 13. Juli 2017 (BGBl. I S. 2347) wurde durch die Ergänzung von Art. 91c GG dem Bund die Möglichkeit gegeben, die elektronische Bereitstellung von Verwaltungsdienstleistungen durch Gesetze voranzubringen bzw. zu regeln. Mit dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsdienstleistungen (**Onlinezugangsgesetz** – OZG) vom 14. August 2017 (BGBl. I S. 3122, 3138) hat der Bundesgesetzgeber mit Zustimmung des Bundesrates davon Gebrauch gemacht.

Der neue Abs. 5 von Art. 91c GG schafft eine ausschließliche Gesetzgebungszuständigkeit des Bundes für die digitale Verwaltung, allerdings mit Zustimmung des Bundesrates: “Der übergreifende informationstechnische Zugang zu den Verwaltungsleistungen von Bund und Ländern wird durch Bundesgesetz mit Zustimmung des Bundesrates geregelt“.

Die zentralen Bestandteile des OZG bilden der bundesweite Portalverbund und das einheitliche Nutzerkonto. Zukünftig sollen Nutzerinnen und Nutzer elektronische Behördendienste zu allen Verwaltungsangelegenheiten über jedes Portal erreichen und erledigen können und sich auf Wunsch nur einmal und einheitlich im Portalverbund und gegenüber allen angeschlossenen Behörden mit Hilfe dieses einheitlichen Nutzerkontos identifizieren.

Der geplante Portalverbund selbst ist aber kein zentrales Portal, sondern vielmehr eine Verknüpfung der Verwaltungsportale der Länder. Dabei soll dieser Portalverbund *mehr* leisten als nur eine „Verlinkung von Online-Angeboten“. Neben dem einheitlichen Nutzerkonto werden einheitliche Kommunikationsschnittstellen und IT-Sicherheitsstandards für alle Verbundteilnehmer vorgeschrieben. Damit wird die Grundlage für eine Vereinheitlichung der IT-Anwendungen der gesamten öffentlichen Verwaltung – also für die „digitale Verwaltung“ im Bund sowie in Ländern *und* Kommunen – gelegt.

Bis Ende des Jahres 2022 müssen alle geeigneten Verwaltungsleistungen von Bund und Ländern online bereitgestellt sowie in Portalen und im übergreifenden Portalverbund nutzbar sein. Die Bürgerinnen und Bürger müssen für alle Leistungen ein einheitliches Nutzerkonto verwenden können. Bereits im April 2016 formulierte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) Forderungen an die datenschutzgerechte Umsetzung solcher Servicekonten (**Anlage 2**).

Im Übrigen enthält das OZG Verordnungsermächtigungen, um dem Bund die Möglichkeit zu geben, für die Anbindung an sowie den Betrieb und die Abwicklung von Verwaltungsleistungen im Portalverbund Festlegungen zu treffen. Danach kann die Bundesregierung durch Rechtsverordnung IT-Anwendungen und Basisdienste sowie die technische Umsetzung von Standards und IT-Sicherheitsvorgaben auch für die Länder vorgeben, soweit sie Bundesrecht ausführen. Solche Verordnungen bedürfen des Benehmens mit dem IT-Planungsrat und der Zustimmung des Bundesrats. Die Länder dürfen durch Landesrecht davon abweichen, sofern sie bereits im Portalverbund geeignete IT-Komponenten bereitstellen.

Das Bundesministerium des Innern, für Bau und Heimat (BMI) kann durch Rechtsverordnung ohne Beteiligung des IT-Planungsrats und *ohne* Zustimmung des Bundesrats die zur Gewährleistung der IT-Sicherheit im Portalverbund erforderlichen Standards festsetzen. Eine Abweichung hiervon ist den Ländern *nicht* erlaubt. Weiterhin kann das BMI durch Rechtsverordnung im Benehmen mit dem IT-Planungsrat und *ohne* Zustimmung des Bundesrats die technischen Kommunikationsstandards innerhalb des Portalverbunds festlegen.

Für die elektronische Abwicklung bzw. die Anbindung konkreter Verwaltungsverfahren an den Portalverbund können mittels Verordnung hingegen Kommunikationsstandards des jeweils fachlich zuständigen Bundesministeriums festgelegt werden (hier im Einvernehmen mit dem BMI, im Benehmen mit dem IT-Planungsrat und mit Zustimmung des Bundesrats). Zukünftig wird also der Bund und nicht mehr der IT-Planungsrat die Vorgaben für Anwendungen, Basisdienste, Sicherheits- und Kommunikationsstandards für die „digitale Verwaltung“ in Bund, Ländern und Kommunen erarbeiten.

Das Konzept der Landesregierung, es den Kommunen zu überlassen, auf freiwilliger Basis zu entscheiden, ob und welche Verwaltungsleistungen sie mit welchen Standards anbieten, war damit gescheitert.

Mit Beschluss vom 16. Mai 2017 hat die Landesregierung den Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung des Landes Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt – EGovG LSA; Stand: 8. Mai 2017) zur Anhö-

rung freigegeben. Der Landesbeauftragte hatte gegenüber dem MI in seiner Stellungnahme vom 16. Juni 2017 erneut auf die Defizite des Gesetzentwurfs hingewiesen und hierzu seine Empfehlungen gegeben.

Der Gesetzentwurf der Landesregierung vom 19. September 2017 (LT-Drs. 7/1877) wurde vom Landtag an den federführenden Ausschuss für Inneres und Sport überwiesen. Dieser führte am 15. März 2018 eine öffentliche Anhörung durch, zu der auch der Landesbeauftragte eingeladen wurde. Einer Empfehlung des Innenausschusses folgend, wurde die Anhörung in drei Teile gegliedert, die in einem 1. Teil grundsätzliche Fragen und die unterschiedlichen Modelle der E-Government-Gesetze im Bundesvergleich betraf. In einem 2. Teil sollten die in Bezug auf die Verwaltungsorganisation zu beachtenden Punkte erörtert und in einem 3. Teil die Auswirkungen auf Unternehmen und sonstige Akteure behandelt werden.

Auf Bitten des Innenausschusses äußerte sich der Landesbeauftragte vorab am 28. Februar 2018 in einer schriftlichen Stellungnahme (7/INN/19, Vorlage 3, Drs. 7/1877, 1. März 2018). Im Rahmen der Anhörung ging der Landesbeauftragte nochmals auf seine bereits in mehreren Stellungnahmen an das MI vorgetragenen Kritikpunkte ausführlich ein:

- Die Bedingungen für ein modernes E-Government-Gesetz für das Land, das die gesamte Verwaltung, insbesondere auch die Kommunen, auf die Digitalisierung vorbereitet und für Unternehmen sowie für die Bürgerinnen und Bürger leicht verständlich ist, erfüllt dieser mit einer fast 3-jährigen Verspätung eingebrachte Gesetzentwurf nicht.

- Die gewählte Gesetzessystematik bzw. Begrifflichkeit ist sowohl für die ausführende Verwaltung als auch für die Nutzer (Unternehmen sowie Bürgerinnen und Bürger) in hohem Maße *anwenderunfreundlich*. Andere Bundesländer regeln den Geltungsbereich bestimmter und verständlicher. Beispielhaft verwies der Landesbeauftragte auf das kürzlich erlassene EGovG des Saarlandes.

- Die Beibehaltung der Regelungssystematik des Gesetzentwurfs mit einer kaum geänderten Verweisung auf das EGovG des Bundes und damit keiner Vollregelung für das Land Sachsen-Anhalt selbst hält der Landesbeauftragte für bedenklich. Der gegenwärtige Gesetzentwurf stellt damit einen Sonderweg Sachsen-Anhalts dar. Alle anderen Bundesländer bevorzugen eine *Vollregelung* in ihren E-Government-Gesetzen. Ein so kompliziertes Gesetz unterstützt nicht im notwendigen Maße die ehrgeizigen Ziele der *Digitalen Agenda* des Landes Sachsen-Anhalt, den digitalen Wandel auch in der Verwaltung erfolgreich zu gestalten.

- Die Gemeinden und Gemeindeverbände sind nach § 1 OZG verpflichtet, ihre Verwaltungsleistungen zukünftig über den Portalverbund anzubieten. Das gilt folglich auch für die kommunale Ebene von Sachsen-Anhalt und müsste damit deutlich im Gesetzentwurf Berücksichtigung finden. Das ist bisher nicht der Fall.

- Ein Kernbestandteil des Gesetzentwurfs, nämlich die *elektronische Aktenführung*, die eigentlich die Basis einer Digitalisierung der Verwaltung darstellt, fin-

det auf die Kommunen keine Anwendung. Auch die Nutzung des Landesportals Sachsen-Anhalt ist für die Kommunen nicht verpflichtend.

- Die Regelungen des EGovG LSA zum Portalverbund müssen gleichermaßen für die unmittelbare und mittelbare Verwaltung des Landes gelten. Die dem Gesetzentwurf zugrundeliegende Differenzierung zwischen der *unmittelbaren* Landesverwaltung (Landesbehörden und Einrichtungen des Landes) und der *mittelbaren* Landesverwaltung, die in weiten Teilen die kommunale Ebene mit Blick auf ihre *Selbstverwaltung* und das *Konnexitätsprinzip* vom Anwendungsbereich des Gesetzes ausnimmt, ist damit nicht mehr haltbar.

Von besonderer Bedeutung für die Entwicklung des Landes gerade in wirtschaftlicher Hinsicht ist der mit der *Digitalen Agenda* der Landesregierung (Beschluss vom 19. Dezember 2017) angestrebte Modernisierungsprozess. Die wichtigsten strategischen Ziele finden sich in einem Zehn-Punkte-Plan wieder, der der Agenda vorangestellt wurde. Im Zusammenhang mit dem Entwurf des EGovG LSA war Nr. 10. besonders relevant:

„10. Wir bauen die öffentliche Verwaltung zu einem digitalen Dienstleister um.
In den kommenden Jahren werden wir die öffentliche Verwaltung zu einem digitalen Dienstleister für die Bürgerinnen und Bürger sowie Unternehmen unseres Landes weiterentwickeln. Als Grundprinzip dient dabei die enge Kooperation zwischen Bund, Ländern und Kommunen. Ausgehend von der IKT-Strategie „Sachsen-Anhalt digital 2020“, dem im Sommer 2017 beschlossenen Onlinezugangsgesetz (OZG), dem im Juli 2018 zu verabschiedenden E-Government-Gesetz des Landes sowie befördert durch die Entwicklungen auf Bundes- und europäischer Ebene wird das Land eine neue E-Government-Strategie verabschieden. Zudem werden wir das Landesportal www.sachsen-anhalt.de (LPSA), das schon heute alle öffentlich verfügbaren Informationen und Dienstleistungsangebote der Landesbehörden bündelt, stetig weiterentwickeln.“

Im Rahmen der mündlichen Anhörung haben sich die kommunalen Spitzenverbände und Vertreter der Wirtschaft der Kritik des Landesbeauftragten angeschlossen. Sie haben die Landesregierung zu einer umfassenden Überarbeitung des Gesetzentwurfs aufgefordert. Sie ziehen eine Vollregelung im Gesetz vor, und verlangen verbindliche Regelungen und Standards für die elektronische Verwaltung in den Kommunen. Das beinhaltet auch die Pflicht zur elektronischen Aktenführung und die Pflicht, alle Verwaltungsleistungen über das Landesportal anzubieten.

Angesichts dieser massiven Kritik und des doch deutlich an die Landesregierung herangetragenen Wunsches einer Überarbeitung des (offensichtlich als misslungen empfundenen) Gesetzesentwurfs wäre es eigentlich zu erwarten gewesen, dass die Landesregierung den Entwurf grundlegend überarbeitet. Die Zeit drängt, denn mit der Einführung des *Elektronischen Rechtsverkehrs* in der Justiz muss spätestens zum *1. Januar 2022* die elektronische Kommunikation in der gesamten Landesverwaltung nicht nur geregelt, sondern auch realisiert sein (vgl. auch Nr. 8.2). Vor diesem Hintergrund ist es nicht nachvollziehbar, dass die Landesregierung in ihrer Stellungnahme vom 7. Juni 2018 zum IV. Tätigkeitsbericht zur Informationsfreiheit vom 21. Juni 2016, in dem der Landesbeauftragte das geplante E-Government-Gesetz aus informationszugangsrechtlicher Sicht erörtert hatte, erklärt hat, an dem Gesetz in

seiner jetzigen Form festhalten zu wollen (LT-Drs. 7/3067, zu Nr. 9.2). Das sollte nicht das letzte Wort sein. Die Entscheidung des Landtages steht aus.

Der Gesetzentwurf ist ein Kernvorhaben der Landesregierung. Ein zukunftsfähiges E-Government bildet eine wesentliche Grundlage für eine moderne Verwaltung in Sachsen-Anhalt und die Digitalisierung in diesem Land. Eine angepasste E-Government-Strategie muss baldmöglichst verabschiedet werden.

Der Landesbeauftragte empfiehlt darüber hinaus dringlich, den Gesetzentwurf grundlegend zu überarbeiten. Dazu bedarf es einer Vollregelung. Die rechtlichen Rahmenbedingungen, die durch das Bundesgesetz zum E-Government und das Onlinezugangsgesetz bereits bestehen, müssen umfänglich Berücksichtigung finden. Die Kernelemente wie die Pflicht zur elektronischen Kommunikation, die Pflicht zur Durchführung elektronischer Verwaltungsverfahren und die Pflicht zur elektronischen Aktenführung gehören in ein solches Gesetz. Dabei müssen die Kommunen verpflichtend einbezogen werden, denn konkrete Verwaltungsleistungen werden nicht von den Ministerien, sondern von den Kommunen vor Ort erbracht.

4.5 IT-Planungsrat – neue Anforderungen erfordern neue Strukturen

Der IT-Planungsrat (IT-PLR) – vgl. XII. Tätigkeitsbericht (Nr. 4.1) – hat im zurückliegenden Berichtszeitraum wesentliche Entscheidungen für die Verwaltungsdigitalisierung zu Schlüsselprojekten, wie dem Portalverbund, dem Digitalisierungsprogramm und der Föderalen IT-Kooperation (FITKO), getroffen. Bereits im März 2016 hatte sich der IT-PLR entschieden, der FITKO einen neuen Rahmen zu geben, um die im IT-Staatsvertrag vorgesehene Steuerungs- und Koordinierungsfunktion wirksamer erfüllen zu können. Hierzu wurde die Bildung einer rechtsfähigen Anstalt des öffentlichen Rechts (AöR) in gemeinsamer Trägerschaft aller Länder und des Bundes mit Sitz in Frankfurt am Main beschlossen. Nach Klärung der Finanzierungsfragen zur AöR soll der IT-Staatsvertrag zum 31. Dezember 2019 geändert werden.

Auf seiner 25. Sitzung am 14. April 2018 hat der IT-PLR seine Arbeitsschwerpunkte für 2018 festgelegt. Auf der Tagesordnung standen zentrale Themen zur Digitalisierung der Verwaltung wie die bürger- und unternehmensfreundliche Gestaltung elektronischer Zugänge, die Umsetzung des Onlinezugangsgesetzes (OZG), das Programm zur Digitalisierung von Bürgerdiensten und das Thema Informationssicherheit.

Ein zentrales Thema war der Portalverbund. Die geplante bürgerorientierte Verbund-Architektur nimmt derzeit Gestalt an. Dazu hatte der IT-PLR in seiner Sondersitzung am 8. Februar 2018 die Grundprinzipien der IT-Architektur für verbindlich erklärt und die pilothafte Errichtung eines Online-Gateways für die Verknüpfung der Portale von Bund und Ländern beschlossen. An diesem Pilotprojekt sind die Länder Bayern, Berlin, Hamburg, Hessen und der Bund beteiligt. Die 91. Datenschutzkonferenz (DSK) hatte hierzu bereits im April 2016 mit einer Entschließung (**Anlage 2**) reagiert. Der IT-PLR hatte sich mit Beschluss vom Juni 2015 für eine flächendeckende Verbreitung sog. Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen.

Die DSK und auch der Landesbeauftragte werden sich mit diesen zentralen Themen der Digitalisierung der öffentlichen Verwaltung in Bund und Ländern in den nächsten Jahren intensiv beschäftigen und diese datenschutzrechtlich wie datenschutztechnisch begleiten.

4.6 Dataport – Fachverfahren Zentraler Meldebestand (ZMB)

Mit dem Inkrafttreten des Staatsvertrages über den Beitritt des Landes Sachsen-Anhalt zum IT-Verbund der nordostdeutschen Länder – Dataport am 24. Februar 2014 (GVBl. LSA S. 94) umfasst dieser IT-Verbund nunmehr sechs Trägerländer. Damit ist für die Landesbeauftragten der Trägerländer eine Abstimmung u. a. bei den Prüfungsmaßstäben, dem Zusammenwirken bei Prüfungen und bei der Beratung erforderlich. Hierzu dienen regelmäßige Treffen der Landesbeauftragten auf Arbeits- und Leitungsebene. Neben den mehrmals im Jahr stattfindenden Besprechungen der IT-Referenten finden unter wechselndem Vorsitz einmal jährlich Treffen der Landesbeauftragten mit dem Dataport-Vorstand statt. Im Jahr 2017 hatte der Landesbeauftragte von Sachsen-Anhalt den Vorsitz dieser Gesprächsrunde inne. Themenschwerpunkte waren u. a. die Gesetzgebungsverfahren zur DS-GVO in den Ländern, die notwendige Anpassung des Dataport-Staatsvertrages an die DS-GVO, aktuelle Entwicklungen im E-Government sowie die bestehenden E-Government-Basisinfrastrukturen von Dataport (vgl. im Übrigen XII. Tätigkeitsbericht, Nr. 4.6).

Für das von Dataport für die Trägerländer Hamburg, Schleswig-Holstein und Sachsen-Anhalt betriebene Fachverfahren „Zentraler Meldebestand“ war erstmalig eine gemeinsame datenschutzrechtliche Kontrolle für März 2017 vereinbart worden.

Das am 1. November 2015 in Kraft getretene Ausführungsgesetz des Landes Sachsen-Anhalt zum Bundesmeldegesetz – BMG-AG LSA vom 21. Juli 2015 (GVBl. LSA S. 369), i. V. m. mit der Verordnung zum Zentralen Meldedatenbestand des Landes Sachsen-Anhalt – ZMDB-VO LSA vom 13. November 2015 (GVBl. LSA S. 565), bilden seit dem 20. November 2015 die Rechtsgrundlage für den Betrieb der Landesinformationsstelle für Meldedaten (§ 2 BMG-AG LSA). Der Zentrale Meldedatenbestand (ZMDB) des Landes Sachsen-Anhalt wird als automatisiertes Verfahren vom Ministerium für Inneres und Sport beim zentralen IT-Dienstleister Dataport in Auftrag gegeben und von Dataport auf einer gemeinsamen IT-Infrastruktur, in der sich auch die Verfahren zu den Zentralen Meldedatenbeständen der Länder Hamburg und Schleswig-Holstein befinden, betrieben (s. Nr. 6.8).

Daher führten die Datenschutzbeauftragten dieser drei Trägerländer eine gemeinsame datenschutzrechtliche Kontrolle des Fachverfahrens „Zentraler Meldebestand (ZMB)“ bei Dataport durch. Schwerpunkt der Prüfung des Fachverfahrens ZMB bildete die Umsetzung der Datensicherheit, insbesondere die Gewährleistung der Vertraulichkeit und der Trennung (Mandantentrennung) des gespiegelten Meldedatenbestandes Sachsen-Anhalts von den übrigen Meldedatenbeständen der anderen beteiligten Länder. Die Überprüfung des Fachverfahrens betraf die Ebenen Web-Anwendung, Datenbank, Netze und Netzwerkspeicher (SAN).

Neben den Vertragsunterlagen zur Auftragsdatenverarbeitung und dem Verfahrensverzeichnis wurden im Vorfeld der Vor-Ort-Kontrolle die Umsetzungsdokumente des Fachverfahrens ZMB für den Bereich Datenbank und Netzwerkspeicher angefordert und auf Vollständigkeit und Konsistenz geprüft. Hierzu gehörten u. a. Dokumente wie

die Prozessbeschreibung, die Risikobetrachtung und -bewertung, das Mandantenkonzept, das Datenschutz- und Datensicherheitskonzept, die Sicherheitsrichtlinien sowie entsprechende Notfallhandbücher.

Das vorgelegte ISO 27001-Zertifikat auf Basis von IT-Grundschutz (BSI-IGZ-0170-2014) war für das Rechenzentrum RZ² bis 24. April 2017 gültig und bildete mit den entsprechenden für die Bereiche Datenbank und Netzwerkspeicher umgesetzten Maßnahmen der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Grundlage für die datenschutzrechtliche Kontrolle. In den Umsetzungsdokumentationen wurden für den Bereich Datenbank und Datenbankmanagementsystem die BSI-Anforderungen zu Authentifizierung, Autorisierung, Sicherheitsfeatures, grundlegende Konfiguration, Audit, Verschlüsselung und Trennung geprüft. Für den Bereich Netzwerkspeicher (SAN) wurden die BSI-Anforderungen zu Vertraulichkeit, Grundkonfiguration und Trennung kontrolliert.

Nachdem fehlende Dokumentationen von Dataport nachgereicht sowie festgestellte Inkonsistenzen in der Dokumentation und offene Fragen vorab mitgeteilt wurden, wurde die gemeinsame Vor-Ort-Kontrolle in einem zweitägigen Termin am Standort Hamburg durch die Datenschutzaufsichtsbehörden der Länder Hamburg, Sachsen-Anhalt und Schleswig-Holstein unter Anwesenheit eines Vertreters der Bremer Datenschutzbeauftragten im März 2017 durchgeführt. Während des Vor-Ort-Termins mussten vereinzelt Nachbesserungsbedarfe in der Organisation und Implementation des Verfahrens festgestellt werden. Nachdem alle verfahrensrelevanten Dokumente seitens Dataport auf den aktuellen Stand gebracht wurden und die Datenschutzbehörden einen gemeinsamen Sachstandsbericht verfasst und Dataport zur Stellungnahme gegeben haben, steht die gemeinsame rechtliche Bewertung des Verfahrensbetriebs ZMB bei Dataport noch aus. Da allerdings bereits im Laufe des Prüfprozesses seitens Dataport kontinuierlich nachgebessert wurde, sind keine wesentlichen Beanstandungen am Verfahren zu erwarten.

4.7 Das Trusted-Cloud-Datenschutzprofil

Trusted Cloud war ein vom Bundesministerium für Wirtschaft und Energie (BMWi) in den Jahren 2010 bis 2015 gefördertes nationales Technologieprogramm zur Entwicklung und Etablierung vertrauenswürdiger Cloud Services in Deutschland. Aus dem Trusted-Cloud-Projekt ging das Pilotprojekt Trusted-Cloud-Datenschutzprofil (TCDP) hervor, welches in zwei Iterationen bis 2016 zum Prüfstandard entwickelt wurde, durch den mittels Zertifizierung nachgewiesen werden kann, dass ein Cloud-Dienst die gesetzlichen Anforderungen des Bundesdatenschutzgesetzes (BDSG) an eine Auftragsdatenverarbeitung erfüllt.

Im Pilotprojekt TCDP wurden die deutschen Aufsichtsbehörden von Anfang an eingebunden. Der Aufruf zur Beteiligung wurde an die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder gerichtet, welche wiederum in ihrem Arbeitskreis Technik freiwillige Teilnehmer gewinnen konnte. Der Landesbeauftragte wurde zum Ende des Projektes aufgenommen.

Der Vertreter des Landesbeauftragten hat in der Taskforce TCDP mitgewirkt. Hierbei ging es darum, den Anforderungskatalog, dem die Zertifizierung zugrunde liegt, auszugestalten und zu verfeinern sowie diesen mit Referenzen auf bereits vorhandene Maßnahmen aus ISO/IEC-Normen zu untersetzen. Dabei wurden konkrete Formulie-

rungsvorschläge unterbreitet und vorhandene Texte aus Datenschutzsicht revisioniert.

Eingeflossen sind hauptsächlich die Anforderungen des BDSG sowie Anforderungen und Maßnahmen aus den ISO/IEC-Normen 27002 (IT-Sicherheit), 27017 (Cloud-Sicherheit) und 27018 (Cloud-Datenschutz). Anforderungen der Datenschutz-Grundverordnung (DS-GVO) sind nicht konkret eingeflossen, da diese während der ersten Hälfte der Projektlaufzeit noch nicht in Kraft getreten war. Jedoch ist das TCDP, wie auch das BDSG, an vielen Stellen kompatibel bzw. deckungsgleich mit der DS-GVO. Andere Standardisierungsbemühungen wurden zur Kenntnis genommen, jedoch über die oben genannten ISO/IEC-Normen hinaus nicht konkret berücksichtigt. Bei widersprüchlichen Anforderungen hatten immer die Anforderungen aus dem BDSG Vorrang.

Für die beteiligten Datenschutzbehörden war es maßgeblich, dass das BDSG vollständig abgebildet wurde. Das ist auch geschehen. Durch das BMWi wurde ein Nachfolgeprojekt zur DS-GVO-Konformität in Aussicht gestellt, an welchem sich der Landesbeauftragte wieder beteiligen würde.

4.8 KV-FlexNet – Zugang zum Sicheren Netz der Kassenärztlichen Vereinigung

Mit dem sog. KV-SafeNet haben die Kassenärztlichen Vereinigungen (KVen) vor Jahren niedergelassenen Ärzten und ärztlichen Einrichtungen einen hardwarebasierten Zugang zum Sicheren Netz der Kassenärztlichen Vereinigungen (SNK) ermöglicht. Die Einrichtung eines entsprechend abgesicherten Routers, der den VPN-Tunnel zum SNK aufbaut, musste mit relativ großem Aufwand durch akkreditierte IT-Dienstleister durchgeführt werden. Somit war es insbesondere kleinen Arztpraxen nicht möglich, eine Anbindung an das SNK einzurichten. Mit der Umstellung auf eine ausschließlich elektronische Abrechnung der Ärzte bei den KVen musste eine softwarebasierte Lösung, die von jedem Arzt und auch auf mobilen Geräten eingesetzt werden kann, geschaffen werden.

Mit der Einführung des sog. KV-FlexNet wurde diese flächendeckende, mobile und softwaregestützte Anbindung niedergelassener Ärztinnen und Ärzte in Sachsen-Anhalt an das SNK geschaffen. Allerdings wurde nicht von Anfang an eine Zwei-Faktor-Authentifizierung mit Hilfe des Yubikeys – das ist ein USB-Dongle, der zusätzlich zum Passwort bereitgehalten werden muss – für die Anmeldung am KV-FlexNet vorgesehen. Auch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren war nicht von Anfang an gewährleistet. Das dem Landesbeauftragten vorgelegte KV-FlexNet-Konzept sah allerdings vor, diese Software-VPN-Lösung 1927 Praxen zur Verfügung zu stellen. Da besondere Arten personenbezogener Daten, wie medizinische Daten, auch einer besonderen Absicherung bedürfen und gemäß Anlage zu § 9 Satz 1 BDSG dem Stand der Technik entsprechenden Verschlüsselungsverfahren zu verwenden waren, bestand dringender Handlungsbedarf und die Implementation musste umgehend an die rechtlichen Anforderungen angepasst werden.

Das für den VPN-Tunnel geplante Verschlüsselungsprotokoll TLS Version 1.0 entsprach nicht den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der technischen Richtlinie TR 02102-2. Darin wird grundsätzlich Ver-

sion 1.2 des TLS-Protokolls empfohlen. Version 1.1 biete zwar noch ausreichende Sicherheit, habe allerdings Nachteile gegenüber Version 1.2. Version 1.0 des TLS-Protokolls kann laut BSI nur in bestehenden Anwendungen übergangsweise weiter eingesetzt werden und ist somit für die Entwicklung neuer Verfahren ungeeignet. Zum zur Herstellung eines VPN-Tunnels notwendigen Schlüsselaustausch wurden im KV-FlexNet-Konzept keine Angaben gemacht. Das BSI empfiehlt in der technischen Richtlinie TR 02102-3 hierfür grundsätzlich die Verwendung von Perfect Forward Secrecy (Diffie-Hellman-Verfahren) gemäß IKE-Protokoll der Version 2 für IPsec-basierte Kommunikation (VPN-Tunnel). Bevor das Vorhaben KV-FlexNet flächendeckend zum Einsatz kam, hatte sich der Landesbeauftragte dafür eingesetzt, dass mindestens die vorgenannten technischen Vorgaben des BSI umsetzt werden.

Der Hinweis auf die Eigenverantwortung des Nutzers bei der Herstellung einer entsprechend abgesicherten Arbeitsumgebung (Laptop, PC) wurde durch die auf den Internetseiten zu KV-FlexNet veröffentlichten Sicherheitsregeln nur unzureichend konkretisiert an die niedergelassenen Ärztinnen und Ärzte weitergegeben. Auch zur Trennung privater Kommunikation auf den mobilen Geräten, die mittels KV-FlexNet angebunden sind, wurden keinerlei Hinweise an die Ärztinnen und Ärzte gegeben.

Nach ausgiebigen Beratungen mit dem Landesbeauftragten hatte die KV Sachsen-Anhalt die bemängelten Punkte nachgearbeitet und konnte das Projekt 2016 erfolgreich in den Produktivstatus überführen. Der Landesbeauftragte wird die ordnungsgemäße Implementierung bei den niedergelassenen Ärztinnen und Ärzten im Rahmen seiner aufsichtsbehördlichen Tätigkeit kontrollieren.

4.9 Verschlüsselung im Landesportal und beim Kontaktformular

In den vergangenen Jahren wies der Landesbeauftragte immer wieder darauf hin, dass das unverschlüsselte Betreiben von Webseiten kein Stand der Technik mehr ist und insbesondere dort, wo personenbezogene Daten genutzt oder erfasst werden, grundsätzlich verschlüsselt werden sollte. In Sachsen-Anhalt wurden erkannte Fälle formal nicht beanstandet, sondern Betreibern wurde die Rechtslage erläutert und es wurde hinsichtlich der Möglichkeiten zur Verschlüsselung beraten. Den Ratschlägen wurde in der Regel gefolgt.

Die Staatskanzlei als Betreiber des Landesportals Sachsen-Anhalt und damit nahezu aller Webseiten von Landesbehörden verwies immer wieder darauf, dass im Portal keine personenbezogenen Daten verarbeitet würden, und wo doch, ja bereits die geforderte Verschlüsselung realisiert würde. Das stimmte größtenteils (Ausnahme Kontaktformular) auch. Die Polizei benutzte bereits verschlüsselte Seiten mit eigenem Verschlüsselungs-Zertifikat, jedoch eingebettet in unsichere Unterseiten des Landesportals. Daraus entstanden Sicherheitslücken, da jetzt sichere Webseiten innerhalb von unsicheren Webseiten angezeigt wurden. Hierdurch wurden aber Angriffe auf die Verschlüsselung der Unterseiten theoretisch ermöglicht.

Das von der Staatskanzlei vorgebrachte Kostenargument gegen eine Verschlüsselung auf dem Webserver – Zertifikate seien zu teuer – konnte widerlegt werden, da ein gemeinsam genutztes Zertifikat für alle preiswerter ist.

Ganz plötzlich – Anfang 2017 – wurde das Landesportal auf TLS 1.2 umgestellt und die damals bereits bereichsspezifisch nutzbare Verschlüsselung wurde für das ge-

samte Landesportal inklusive dem Kontaktformular freigeschaltet. Damit geht Sachsen-Anhalt nun mit gutem Beispiel voran. Wurde bislang z. B. von einem Unternehmer eine sichere Webpräsenz verlangt, konnte dieser immer darauf verweisen, dass das Land sich selbst nicht (überall) an die Vorgaben des Landesbeauftragten hält.

Webseiten sind jedoch nicht nur dann zu verschlüsseln, wenn personenbezogene Daten über Web-Formulare erhoben werden. Auch anfallende Logdaten, von Dritten einsehbare Datenübertragungen (z. B. im öffentlichen WLAN), ja selbst die DNS-Anfragen sind personenbezogen auswertbar und damit nach dem Stand der Technik zu schützen.

Verschlüsselung ist Stand der Technik und nach Art. 5 i. V. m. Art. 25 und 32 DS-GVO anzuwenden. Das gilt auch dann, wenn keine personenbezogenen Daten vom Portal verwendet werden, da auch anfallende Inhalts-, Zugriffs- und Logdaten zumindest personenbeziehbar sind.

4.10 Sicherheit bei Web-Anwendungen und Portalen

Immer wieder musste der Landesbeauftrage hinsichtlich der Notwendigkeit der Verschlüsselung von Webseiten, der Sicherheit von X.509-Zertifikaten und der auszuwählenden Parameter dieser Zertifikate beraten. Insbesondere durch fehlerhaft ausgestellte Zertifikate einiger großer Zertifizierungsstellen (Certificate Authorities – CAs) herrschte Unsicherheit, ob man Zertifikate bestimmter Anbieter noch nutzen darf oder ob die anderer Anbieter „besser“ sind.

Zertifikate deutscher Internetanbieter stammen oft von Dritten betriebenen CAs. So wurde angefragt, ob ein Zertifikat eines solchen Anbieters ausreichend wäre. Dieser verkaufte Zertifikate von Symantec und GeoTrust, ein anderer die von Thawte. Bei der Ausstellung von Zertifikaten können immer wieder Pannen passieren und CAs in die Schlagzeilen geraten. Unternehmen werden umbenannt oder verkauft. Es ist schwer, pauschal zu sagen, ob ein Anbieter geeignet ist oder nicht. Als groben Check, ob ein Anbieter vertrauenswürdig ist, sollte eine Suchmaschine befragt werden (Datenpannen, Herkunftsland, Policies, Webseite der CA) und auch getestet werden, ob die Hersteller der großen Webbrowser und Betriebssysteme die Wurzel-CAs dieser Anbieter hinterlegt haben. Wenn die CA dann auch noch von einem deutschen Provider angeboten oder selbst genutzt wird, kann kaum mehr zur Überprüfung getan werden. Letztlich greift auch die Landes-PKI bei besonderen Anforderungen auf die Produkte eines Dritten (z. B. TeleSec ServerPass Standard) zurück.

Bei der Prüfung von HTTPS-verschlüsselten Webseiten wurden oft Defizite festgestellt, die sich aber meist einfach beheben ließen. So wurde beispielsweise eine Website hinsichtlich der genutzten Zertifikate geprüft und dabei festgestellt, dass unsichere Algorithmen genutzt wurden (MD5/SHA1-Hashes). Da das Zertifikat kurz vor der Erneuerung stand und von einem großen Anbieter kam, der in neueren Zertifikaten bereits nachgebessert hatte, wurde geraten, nur darauf zu achten, dass bei der Aktualisierung aktuelle Algorithmen genutzt werden. Eine andere Website – eine Kitaplatz-Verwaltung – nutzte eine reduzierte Schlüsselgröße und Zertifikate eines großen amerikanischen Anbieters. Über die Ursachen solcher schwachen Zertifikate – Absicht? US-Exportbestimmungen? – kann nur spekuliert werden. Auch hier hatte der Anbieter mittlerweile ausreichend lange Schlüssel im Angebot, sodass geraten

wurde, beim sowieso in naher Zukunft geplanten Austausch darauf zu achten, dass Zertifikate nach dem Stand der Technik installiert werden.

Den Landesbeauftragten erreichten auch Anfragen zur Transportverschlüsselung nach dem Transport-Layer-Security-Protokoll (TLS) – soll die Version 1.0, 1.1 oder 1.2 genutzt werden? TLS 1.2 stammt aus dem Jahr 2008 und sollte eigentlich Mindeststandard sein. Hinzu kommt aber, dass mittlerweile auch Verfahren und Algorithmen aus TLS 1.2 überholt sind und nicht mehr genutzt werden sollten. So riet der Landesbeauftragte immer zu mindestens TLS 1.2 und weiteren Vorgaben (aus dem Entwurf zu TLS 1.3 – u. a. kein MD5, RC4, SHA1, …) mit dem Ziel, zumindest die sichere Nutzung für die, die es wollen, zu ermöglichen und allen anderen – sofern notwendig – die ältere TLS-Version zu erlauben.

Auch das BSI traf hierzu widersprüchliche Aussagen. So hatte das BSI bereits 2013 einen Mindeststandard zur TLS-Nutzung herausgegeben, der TLS 1.2 in Verbindung mit Perfect Forward Secrecy (PFS) für Bundesbehörden empfiehlt. Auch in der Technischen Richtlinie TR-02102-2 „Verwendung von TLS“ wird TLS 1.2 empfohlen. Dann ging das BSI aber soweit, TLS 1.0 sogar zu verbieten („darf nicht mehr eingesetzt werden“). Das war 2015 und aus Sicherheitsgründen ist das gar nicht anders formulierbar. In der Praxis funktioniert das in hochgradig heterogenen Umgebungen mit vielen Nutzern und Anwendungen jedoch nicht und so wurde TLS 1.2 – wenn überhaupt – immer in Verbindung mit älteren TLS-Standards angeboten. Mittlerweile steht in der TR-02102-2 bei TLS 1.0 „wird nicht empfohlen“. Aber richtig durchgesetzt hat sich TLS 1.2 bis heute nicht.

Das soll nun der TLS 1.3-Standard schaffen, der neben mehr Geschwindigkeit vor allem mehr Sicherheit bringt. TLS 1.3 ist prinzipiell fertig und nutzbar und wird zu signifikanten Verbesserungen der Internet-Sicherheit führen. Insbesondere unter den Altlasten wurde aufgeräumt (gestrichen wurden u. a. Export Ciphers, MD5, SHA1, RC4, AES CBC-Mode, RSA, MAC-then-Encrypt). Für den Nutzer gibt es einen deutlich schnelleren und sichereren Verbindungsaufbau. So wird jetzt die „Authenticated Encryption“ genutzt und der symmetrische Sitzungsschlüssel wird nicht mehr via RSA ausgetauscht, sondern nur noch durch das Diffie-Hellman-Verfahren, möglichst unter Nutzung von elliptischen Kurven (ECDHE). Dadurch sind bei Verlust eines Serverschlüssels alte Inhalte nicht nachträglich entschlüsselbar (PFS). Jedoch stellte sich heraus, dass noch zu viele Verbindungen abgebrochen werden, da „Mittelboxen“ einiger Hersteller Probleme bereiteten und damit auf unbestimmte Zeit die Einführung des neuen Standards verhindern. Mittelboxen haben hier nichts mit Man-in-the-middle-Angriffen zu tun. Gemeint sind Geräte im Netzwerk, die den verschlüsselten Netzwerkverkehr aufbrechen, verändern oder blockieren (u. a. NAT, Virenscanner, IDS, DLP-Systeme, Firewalls, Proxies, Netzwerkfilter mit Deep Packet Inspection) und damit die Verschlüsselung erschweren.

Viele Zertifikate waren auch offensichtlich unzureichend, also z. B. bereits abgelaufen, selbst erstellt oder auf völlig andere Domainnamen ausgestellt. Solche Fehler müssen in der heutigen Zeit nicht mehr auftreten. Es gibt alternativ auch die Möglichkeit, kostenfrei Zertifikate zu erhalten, die den aktuellen gesetzlichen Anforderungen entsprechen („sicher sind“) und auch von den Webbrowsern ohne Warnungen akzeptiert werden (z. B. von der Let’s Encrypt CA).

Im Zeitraum des Tätigkeitsberichts begannen einige Browserhersteller, Warnungen bei unverschlüsselt zu übertragenden Formularen einzublenden. Das erhöhte den Druck auf die Portalbetreiber, hier aktiv zu werden. Ob es nur daran lag oder andere Gründe dominierten, jedenfalls wurden in genau diesem Zeitraum einige große Websites nachgebessert, sodass der Landesbeauftragte gar nicht mehr einschreiten musste. Das betraf auch eine große Magdeburger Tageszeitung. Der Landesbeauftragte begrüßt ausdrücklich die Initiativen der Browserhersteller zur Verbesserung von Datenschutz und Datensicherheit im Internet, denn es zeigt sich, dass durch ein gemeinsames Vorgehen bei der Einführung von die Sicherheit verbessernden Standards allen Nutzern sehr schnell geholfen werden kann.

Die Verschlüsselung von Webdatenströmen mit mindestens TLS 1.2 (ehem. SSL) ist bezahlbar und Stand der Technik und war damit nach § 6 Abs. 1 DSG LSA zur Absicherung der Übertragung von personenbezogenen Daten verpflichtend zu nutzen. Die seit dem 25. Mai 2018 anzuwendende Datenschutz-Grundverordnung bezieht sich in den Art. 5 i. V. m. Art. 25 und 32 gleichfalls auf den Stand der Technik. Zertifikate „großer" CAs, die in den gängigen Webbrowsern hinterlegt sind, können genutzt werden, ebenso kostenfreie Zertifikate der Let's-Encrypt-Initiative und natürlich auch Zertifikate (Dritter), die von großen deutschen Internet-Unternehmen angeboten werden. Die Transportverschlüsselung sollte immer als TLS 1.3 implementiert bzw. konfiguriert werden. Ältere Versionen sollten nur nach Risikoabwägung mit Bedacht verwendet und nach und nach deaktiviert und durch den aktuellen Standard ersetzt werden.

4.11 Warum die Landesverwaltung Transportverschlüsselung für E-Mails benötigt

Bereits in seinem XII. Tätigkeitsbericht verwies der Landesbeauftragte in Nr. 4.5 auf die (Un)-Möglichkeiten der vertraulichen elektronischen Kommunikation bei der Landesverwaltung unter Nutzung üblicher Verschlüsselungsverfahren. Eine eventuelle Nachrüstung der weit verbreiteten Transportverschlüsselung TLS bei den Landes-E-Mail-Servern wurde dem Landesbeauftragten damals seitens des Ministeriums der Finanzen frühstens mit Einführung des ITN-XT im Jahre 2018 in Aussicht gestellt. Jedoch verzögert sich die Implementierung des ITN-XT weiterhin (s. Nr. 4.2).

Jedoch wird die Herstellung von Vertraulichkeit auch und gerade bei elektronischer Kommunikation durch die Datenschutz-Grundverordnung (DS-GVO) explizit gefordert. Gemäß Art. 5 Abs. 1 lit. f DS-GVO *müssen* personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung.

Gemäß Art. 24 Abs. 1 DS-GVO *muss* der für die Verarbeitung Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt.

Gemäß Art. 32 Abs. 1 DS-GVO *müssen* die zu treffenden technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik ggf. unter an-

derem die Verschlüsselung personenbezogener Daten und die Fähigkeit, die Vertraulichkeit im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, einschließen.

Bei der Beurteilung eines angemessenen Schutzniveaus sind gemäß Art. 32 Abs. 2 DS-GVO die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch unbefugte Offenlegung (ob unbeabsichtigt oder unrechtmäßig) von bzw. durch unbefugten Zugang zu personenbezogenen Daten, die übermittelt wurden.

In der Praxis müssen daher personenbezogene Daten, deren Offenlegung oder unbefugter Zugang der Selbstbestimmung oder dem Ansehen der betroffenen Person schaden kann, durch technische und organisatorische Maßnahmen abgesichert werden. Dafür kann eigentlich nur die Datenverschlüsselung vor oder während der elektronischen Übertragung in Betracht kommen. Denn in einer unverschlüsselten E-Mail werden etwaige Daten vollkommen ungeschützt in einem von jedermann lesbaren Klartextformat (ASCII, TXT, PDF, DOCX, XLSX usw.) mit öffentlichen und umfänglich bekannten Protokollen (TCP/IP, SMTP) über eine nicht bekannte Route in einem weltweiten Netzwerk (Internet) transportiert. Diese Rahmenbedingungen genügen nicht den o. g. Anforderungen der DS-GVO. Das Versenden einer unverschlüsselten E-Mail mit personenbezogenen Daten ohne Umsetzung irgendeiner Sicherheitsmaßnahme ist daher unzulässig.

Vermeintlich ist jedoch das Versenden von E-Mails, in deren Anhang die zu übermittelnden Daten sicher verschlüsselt sind (Ende-zu-Ende-Verschlüsselung mittels OpenPGP oder S/MIME), eine unzumutbare Hürde. Dabei wird oft übersehen, dass eine sichere Datei-Verschlüsselung durch die Vergabe eines Passwortes auf eine Office-Datei, eine PDF-Datei oder auf ein ZIP-Archiv realisiert werden kann[2] – zumindest für einen Übergangszeitraum, bis benutzerfreundliche Verfahren flächendeckend zur Verfügung stehen. Dabei sollte das Passwort unbedingt aus gemischten Zeichen bestehen und eine gewisse Mindestlänge haben, die sich nach dem Stand der Technik richtet, um Wörterbuchattacken und Brute-Force-Angriffen standhalten zu können. Nach Rückmeldungen lässt sich jedoch auch für diesen Ansatz kaum Akzeptanz innerhalb der unmittelbaren Landesbehörden finden, da im Erstellen der ZIP-Archive mit speziellen Programmen und Verabreden der Passwörter per Telefon unnötige Aufwände vermutet werden.

Eine generelle Transportverschlüsselung allen E-Mail-Verkehrs, wie z. B. innerhalb des Providerkooperationsverbundes „E-Mail made in Germany“, wäre der kleinste gemeinsame Nenner, praktisch eine Basisabsicherung um den Anforderungen der DS-GVO im Mindesten gerecht zu werden. In Zukunft ließe sich dann eine flächendeckende Transportverschlüsselung durch weitere Sicherheitsstandards härten. Bei TLS 1.3 werden z. B. nur noch aktuelle und sichere Krypto- und Hashalgorithmen zulässig sein oder mit Techniken wie DANE (DNS-Based Authentication of Named Entities) können die E-Mail-Eingangsserver mittels per DNSSEC hinterlegten Signaturen prüfen, ob eingehende verschlüsselte Verbindungen aus zuverlässigen Quellen stammen. Einige E-Mail-Provider unterstützen bereits derlei zusätzliche Absiche-

[2] Alle drei Varianten basieren auf dem vom BSI anerkannten Verschlüsselungsverfahren AES256, wenn aktuelle Software-Produkte eingesetzt werden.

rungsmethoden und definieren damit den Stand der Technik, welcher von der DS-GVO explizit gefordert wird, neu.

Leider wird selbst die einfache Transportverschlüsselung von den E-Mail-Servern des Landes nicht unterstützt. Das heißt jedoch in der Praxis, dass die E-Mail eines Absenders, der sich von einem TLS-fähigen E-Mail-Provider[3] aus an eine Landesbehörde wendet, entweder nicht zugestellt werden kann (bei Verwendung der Option „TLS erzwingen“) oder zwangsweise unverschlüsselt übertragen wird (bei Verwendung der Option „STARTTLS“), obwohl der Absender durch Wahl eines TLS-fähigen Providers und Konfiguration seines E-Mail-Clients explizit Maßnahmen ergriffen hat, um eine vertrauliche elektronische Kommunikation zu ermöglichen. Somit tritt die Landesverwaltung durch ihre Untätigkeit als Verhinderer geeigneter Schutzmaßnahmen gegenüber Bürgern und Unternehmen in Erscheinung. Gleiches gilt für viele mittelbare Landesbehörden und Kommunen, die bereits auf TLS-fähige Provider umgestellt haben, jedoch die elektronische Kommunikation mit den unmittelbaren Landesbehörden wie Ministerien gezwungenermaßen unverschlüsselt durchführen müssen.

Bei personenbezogenen Daten, bei denen eine gewisse Eintrittswahrscheinlichkeit oder Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu erwarten ist, ist die verschlüsselte E-Mail – vergleichbar mit einem verschlossenen Brief – unverzichtbar. Das besondere elektronische Behördenpostfach und DE-Mail würden ebenfalls eine sichere Alternative zur unverschlüsselten E-Mail darstellen, vor allem was die Integrität und Authentizität elektronischer Nachrichten betrifft.

Immerhin ist im Entwurf des Gesetzes zur Förderung der elektronischen Verwaltung des Landes Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt – EGovG LSA; LT-Drs. 7/1877) in den §§ 11 und 12 die Pflicht zur elektronischen Kommunikation und darüber hinaus in § 9 die Pflicht zur kryptografischen Verschlüsselung dieser elektronischen Kommunikation vorgesehen. Die verschlüsselte elektronische Kommunikation wird somit in absehbarer Zeit zur gesetzlichen Verpflichtung, ohne dass aber vorab eine entsprechende Infrastruktur zur Verfügung steht.

Die unmittelbaren Landesbehörden wären nun eigentlich gezwungen, sich selbst abseits von Landesnetz und Landes-E-Mail-Servern bei externen Providern um Dienste mit verschlüsselter, elektronischer Kommunikation zu bemühen, um aktuellen EU-rechtlichen und kommenden landesgesetzlichen Anforderungen gerecht werden zu können.

Es besteht also dringender Handlungsbedarf für das zuständige Ministerium der Finanzen (ggf. im Zusammenwirken mit Dataport). Die tatsächlichen Dilemmata und die rechtlichen Vorgaben der DS-GVO lassen eine weitere Untätigkeit (s. nochmals XII. Tätigkeitsbericht, Nr. 4.5, mit Hinweis u. a. auf LT-Drs. 6/4299) nicht zu.

[3] Dies lässt sich auf der Seite https://de.ssl-tools.net/mailservers überprüfen.

Für eine verschlüsselte Zurverfügungstellung elektronischer Kommunikationswege muss die Landesverwaltung auf ihren E-Mail-Servern das TLS-Protokoll aktivieren und die baldige Bereitstellung von DE-Mail-Zugängen und des besonderen elektronischen Behördenpostfachs (s. Nr. 8.2) voranbringen.

4.12 Microsoft Cloud-Dienste – „Microsoft Cloud Deutschland“

Im Zusammenhang mit der Bildungspartnerschaft mit Microsoft (u. a. Einkauf von Programmlizenzen; siehe unten Nr. 9.2.5) wurde problematisiert, dass die vielfältigen und vernetzten Angebote von Microsoft nicht mehr auf den jeweiligen Rechner heruntergeladen werden, sondern die Lizenz zur Nutzung von multifunktionalen Angeboten in der Cloud berechtigt. Eine Speicherung von vielfach sensiblen Daten auf Cloud-Systemen großer amerikanischer Anbieter begegnete in datenschutzrechtlicher Hinsicht jedoch noch Bedenken.

Microsoft hat daher die sog. „Deutschland-Cloud“ eingerichtet. Zwei Rechenzentren in Deutschland (Frankfurt/Main und Biere/bei Magdeburg) bieten Cloud-Dienste wie Azure und Office 365 sowie entsprechende Speicherkapazitäten an und gewährleisten die Funktionalitäten nur über diese Systeme. Die Einrichtungen und Programme stehen zwar im Eigentum von Microsoft, der Zugriff auf die Daten ist Microsoft jedoch grundsätzlich verwehrt. Dies wird durch die Einschaltung eines deutschen Datentreuhänders als Betreiber der Einrichtungen bewirkt, sodass auch eventuelle Verpflichtungen Microsofts gegenüber amerikanischen Behörden nicht zum Zuge kommen sollen. Die Datenverarbeitung soll so dem strengen europäischen und deutschen Datenschutzrecht unterliegen.

Die Kontrolle des Zugriffs auf die Daten und Programme für die deutschen Kunden erfolgt durch den Treuhänder, die T-Systems International GmbH. Ein Zugang ist nur direkt für die Kunden bzw. durch einen Zugangssupport von T-Systems International GmbH auf Wunsch des Kunden oder für bestimmte technische Maßnahmen ohne Zugang zu verschlüsselten Kundendaten vorgesehen.

Hinsichtlich der vertraglichen Ausgestaltung zwischen den Kunden und der T-Systems International GmbH ergaben sich seitens der Gremien der Datenschutzkonferenz noch juristische und insbesondere technische und organisatorische Nachfragen, die in mehreren Veranstaltungen und in umfangreichem Schriftverkehr mit Microsoft erörtert wurden, so etwa zur Verhinderung von unbefugten Zugriffen auf die Daten der deutschen Kunden. Demgemäß konnte die Nutzung der „Deutschland-Cloud“ noch nicht abschließend umfassend empfohlen werden. Die Zukunft dieser Cloud-Lösung ist offen.

5 Telekommunikation und Medien

5.1 E-Privacy-Verordnung

Nach den ursprünglichen Plänen der Europäischen Kommission sollte gleichzeitig mit der Anwendung der Datenschutz-Grundverordnung (DS-GVO) die E-Privacy-Verordnung in Kraft treten. Ein erster Entwurf wurde erst am 10. Januar 2017 vorgelegt. Die E-Privacy-Verordnung (Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur

Aufhebung der Richtlinie 2002/58/EG) soll die bislang geltende E-Privacy-Richtlinie (Richtlinie 2002/58/EG), ergänzt durch die sog. Cookie-Richtlinie (Richtlinie 2009/136/EG), ablösen.

Der EU-Gesetzgeber beabsichtigt damit, die DS-GVO im Bereich der elektronischen Kommunikation zu präzisieren und zu ergänzen. Die E-Privacy-Verordnung soll sich aber nicht mehr nur an die klassischen Telekommunikationsanbieter richten, sondern auch an Anbieter sog. „Over-the-Top"-Dienste (OTT) wie Voice over IP, Instant-Messaging und webgestützter E-Mail-Dienste, die ihre Daten über das Internet bereitstellen und daher unabhängig von eigener Infrastruktur oder einem entsprechenden Diensteanbieter sind.

Die wesentlichen Regelungsinhalte der Entwurfsfassung betreffen neben diesen OTT-Diensten auch vernetzte Geräte, Cookies und Web-Tracking, Offline-Tracking und die Direktwerbung. Für den Einsatz von Cookies und sonstigen Tracking-Methoden sind erhebliche Änderungen zu erwarten. Der Entwurf sieht für diesen Bereich das Verbot mit Erlaubnisvorbehalt vor. Demnach soll die Nutzung der Daten von Endgeräten nur erlaubt sein, wenn der Nutzer eingewilligt hat.

Eine weitere wichtige Regelung der Entwurfsfassung ist das Verbot von Offline-Tracking, also das Verbot, Bewegungsprofile etwa durch Verfolgung der Bluetooth-Signale eines Smartphones zu erstellen. Dieses soll ebenfalls nur erlaubt sein, wenn der Nutzer eingewilligt hat. Auch die Direktwerbung mittels elektronischer Kommunikationsdienste, insbesondere per E-Mail, soll grundsätzlich nur noch mit Einwilligung des Nutzers möglich sein. Eine Ausnahme erlaubt Direktwerbung nur bei bestehender Kundenbeziehung; auf die Möglichkeit des Widerspruchs muss hier klar und deutlich hingewiesen werden. Des Weiteren sieht der Entwurf vor, dass Anbieter von Kommunikationsdiensten sicherstellen müssen, dass die verschlüsselte Kommunikation ihrer Nutzer vor unbefugtem Zugriff geschützt wird und nur diese selbst die Möglichkeit haben, die Inhalte wieder zu entschlüsseln.

Im Rahmen europäischer Gesetzgebungsvorhaben werden oft auch durch Interessenverbände Forderungen geltend gemacht. So führt der große Widerstand vor allem aus der Werbewirtschaft, aber auch von Verlagen, dazu, dass mit einem Inkrafttreten der E-Privacy-Verordnung im Jahr 2018 nicht mehr zu rechnen ist. Da diese die Regelungen des Telemediengesetzes (TMG) jedoch zu einem Großteil ersetzen sollte, entsteht infolge der Verzögerung die Frage, ob die datenschutzrechtlichen Regelungen des TMG wegen des Anwendungsvorrangs der DS-GVO überhaupt weiterhin anwendbar sind.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat sich dazu wie folgt positioniert: Die datenschutzrechtlichen Vorschriften des TMG sind seit dem 25. Mai 2018 nicht mehr anwendbar. Zwischenzeitlich unmittelbar geltend, verdrängt die DS-GVO nationales Recht der Mitgliedstaaten. Davon ausgehend haben die Aufsichtsbehörden insbesondere auch ihr Vollzugsverständnis

im Zusammenhang mit Reichweitenmessungen und dem Einsatz von Tracking-Mechanismen in einem Positionspapier[4] dargelegt.

Da dieses Positionspapier von der interessierten Öffentlichkeit strittig diskutiert wurde, hat die DSK im Rahmen einer Anhörung einschlägige Wirtschaftsverbände dazu eingeladen, zur Umsetzung der Positionsbestimmung Stellung zu nehmen – insbesondere zu Fragen der Ausgestaltung im praktischen Vollzug. Die Auswertung dieser Stellungnahmen bleibt abzuwarten.

5.2 Netzwerkdurchsetzungsgesetz

Das Netzwerkdurchsetzungsgesetz, welches am 1. Oktober 2017 in Kraft getreten ist (BGBl. I S. 3352), verpflichtet Anbieter sozialer Netzwerke mit mindestens zwei Millionen registrierten Nutzern, offensichtlich rechtswidrige Inhalte, die auch personenbezogene Daten enthalten können, innerhalb von 24 Stunden nach Eingang einer Beschwerde zu löschen oder zu sperren. Für die Prüfung anderer gemeldeter Inhalte wird den Netzwerkbetreibern eine Frist von sieben Tagen nach Eingang der Beschwerde eingeräumt.

Die 7-Tage-Frist kann überschritten werden, wenn der Netzwerkbetreiber die Entscheidung über die Rechtswidrigkeit innerhalb dieser Frist an eine sog. anerkannte Einrichtung der Regulierten Selbstregulierung abgibt und sich deren Entscheidung unterwirft. Die anerkannte Einrichtung muss dann ihrerseits innerhalb von 7 Tagen über die Rechtswidrigkeit des gemeldeten Inhalts entscheiden. Die Entscheidung über die Anerkennung einer Einrichtung der Regulierten Selbstregulierung wird durch das Bundesamt für Justiz getroffen.

Rechtswidrige Inhalte müssen vor der Löschung zu Beweiszwecken gesichert werden. Deshalb sind Anbieter sozialer Netzwerke verpflichtet, die zu löschenden Inhalte für die Dauer von zehn Wochen aufzubewahren und sie für Zwecke der Strafverfolgung zur Verfügung zu stellen.

Anbieter sozialer Netzwerke, die im Kalenderjahr mehr als 100 Beschwerden über rechtswidrige Inhalte erhalten, sind verpflichtet, halbjährlich einen Bericht über den Umgang mit diesen Beschwerden zu erstellen und im Bundesanzeiger sowie auf der eigenen Homepage zu veröffentlichen. Außerdem müssen Anbieter sozialer Netzwerke ein wirksames und transparentes Verfahren zum Umgang mit Beschwerden vorhalten. Dieses muss für die Nutzer leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein.

Unter anderem stellen die vorsätzliche oder fahrlässige Nichteinhaltung der Berichtspflicht und die Zuwiderhandlung gegen die Pflicht, ein wirksames Beschwerdemanagement vorzuhalten, eine Ordnungswidrigkeit dar. Diese kann mit einer Geldbuße bis zu 5 Millionen Euro geahndet werden. Das Höchstmaß beträgt allerdings 50 Millionen Euro, wenn die Geldbuße gegen juristische Personen und Personenvereinigungen festgesetzt wird (vgl. § 30 Abs. 2 Satz 3 Ordnungswidrigkeitengesetz).

---

[4] http://lsaurl.de/DSKPositionTMG

Die Ordnungswidrigkeit bezieht sich dabei hinsichtlich des Beschwerdemanagements auf die vom Gesetz vorgegebenen Organisationspflichten und nicht auf den einzelnen Löschvorgang. Dem Anbieter eines sozialen Netzwerks droht daher bei einer Fehlentscheidung im Einzelfall kein Bußgeld.

Kritiker befürchten allgemein, dass im Zweifelsfall eher zu viele und damit auch rechtmäßige Inhalte entfernt werden, wodurch ein Eingriff in das Grundrecht auf Meinungsfreiheit erfolgen könne; hierin wird eine unzulässige Zensur gesehen. Außerdem wird bemängelt, dass die Rechtsdurchsetzung nicht durch eine staatliche Stelle vorgenommen, sondern in die Hände von Privatunternehmen gelegt wird. Die EU-Kommission setzt weiterhin auf freiwillige Löschungen.

5.3 Sind IP-Adressen personenbezogene Daten?

Bereits in seinem XII. Tätigkeitsbericht (Nr. 5.5) berichtete der Landesbeauftragte darüber, dass der Bundesgerichtshof (BGH) in einem Rechtsstreit zu klären hatte, ob die Bundesregierung die IP-Adressen ihrer Webseiten-Besucher auch über den Nutzungsvorgang hinaus speichern darf, um Angriffe auf die Web-Server abzuwehren und Angreifer so besser strafrechtlich verfolgen zu können.

Im Oktober 2014 hatte der BGH per Beschluss den Europäischen Gerichtshof (EuGH) um Klärung gebeten, ob IP-Adressen nach europäischem Datenschutzrecht personenbezogene Daten sind. Außerdem sollte geklärt werden, ob die europäische Datenschutzrichtlinie im deutschen Recht die Regelung ermöglicht, wonach eine Speicherung von IP-Adressen über den Nutzungsvorgang hinaus zu Zwecken der Systemsicherheit nicht zulässig ist.

Mit dem Urteil vom 19. Oktober 2016 (Az.: C-582/14, NJW 2016, 3579) hat der EuGH zunächst entschieden, dass die dynamische IP-Adresse eines Nutzers, die beim Zugriff auf eine Webseite gespeichert wird, für den Anbieter der Webseite ein personenbezogenes Datum darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen.

Der EuGH führte hierzu aus, dass es in Deutschland rechtliche Möglichkeiten gibt, die es dem Anbieter einer Webseite erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und anschließend die Strafverfolgung einzuleiten.

In seinem Urteil stellte der EuGH außerdem fest, dass § 15 Abs. 1 Telemediengesetz (TMG) gegen EU-Recht verstößt. Dieser Vorschrift zufolge dürfen Webseiten-Betreiber personenbezogene Daten ihrer Nutzer – also auch deren IP-Adresse – nur speichern, wenn sie für die Inanspruchnahme der Webseite oder zur Abrechnung erforderlich sind. Dies war mit Art. 7 lit. f der EU-Datenschutzrichtlinie 95/46/EG nicht vereinbar. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Diese Abwägung fehlt im TMG.

Nach Beantwortung der Fragen durch den EuGH hat der BGH mit Urteil vom 16. Mai 2017 über die Revisionen der Parteien entschieden. Diese hatten Erfolg und führten zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das Berufungsgericht, das nun entscheiden muss, ob die deutschen Ministerien ein berechtigtes Interesse an der IP-Adressen-Speicherung haben oder die Interessen der Nutzer überwiegen. Die DS-GVO enthält jedenfalls bezüglich der Rechtmäßigkeit der Datenverarbeitung in Art. 6 Abs. 1 lit. f eine ähnliche Bestimmung, in der ebenfalls eine Abwägung zwischen den Interessen des für die Datenverarbeitung Verantwortlichen und der durch die Datenverarbeitung betroffenen Person vorzunehmen ist.

5.4 WLAN-Störerhaftung abgeschafft

Bisher konnten Betreiber öffentlicher WLAN-Hotspots für Urheberrechtsverletzungen, die ihre Nutzer begangen hatten, auf Schadenersatz oder Unterlassung in Anspruch genommen werden. Mit dem Dritten Gesetz zur Änderung des Telemediengesetzes (TMG), welches am 13. Oktober 2017 in Kraft getreten ist, wurde diese Störerhaftung abgeschafft (BGBl. I S. 3530).

Außerdem wurde klargestellt, dass Betreiber öffentlicher WLAN-Hotspots nicht für die gerichtlichen oder außergerichtlichen Kosten der Durchsetzung von Urheberrechten aufkommen müssen. Darüber hinaus dürfen sie nicht von einer Behörde dazu verpflichtet werden, ihr WLAN mit einem Passwort zu schützen oder Nutzer zu registrieren. Die dauerhafte Abstellung des WLANs darf ebenfalls nicht angeordnet werden. Es bleibt WLAN-Betreibern jedoch unbenommen, auf freiwilliger Basis auch weiterhin eine Identifizierung ihrer Nutzer sowie die Eingabe eines Passworts zu verlangen.

Um das geistige Eigentum trotzdem angemessen zu schützen, können Rechteinhaber von WLAN-Betreibern die Sperrung einzelner konkret benannter Internetseiten verlangen, über die ein Nutzer urheberrechtlich geschützte Inhalte illegal verbreitet hat. Damit soll die Wiederholung der Rechtsverletzung verhindert werden. Voraussetzung für diese Sperrung ist, dass der Rechteinhaber im konkreten Fall nur so die Verletzung seines Rechts abstellen kann.

In einem Urteil vom 26. Juli 2018 (I ZR 64/17) hat der Bundesgerichtshof (BGH) die Neuregelung der Störerhaftung bestätigt. Verhandelt wurde ein Fall aus dem Jahr 2013 gegen den Betreiber mehrerer offener WLANs sowie zweier Tor-Exit-Nodes. Nachdem jemand über den Internetanschluss des Beklagten in einer Internet-Tauschbörse verbotenerweise ein Computerspiel zum Herunterladen angeboten hatte, wurde der WLAN-Betreiber vom Rechteinhaber abgemahnt.

Der BGH bestätigte nun in seiner Entscheidung, dass Internetnutzer, die ihr WLAN für die Allgemeinheit öffnen, künftig nicht mehr für fremde Taten auf Unterlassung oder Schadenersatz verklagt werden können. Allerdings legte er den Begriff der „Sperrung“ gem. § 7 Abs. 4 TMG wesentlich weiter aus: „Der Anspruch auf Sperrmaßnahmen ist nicht auf bestimmte Sperrmaßnahmen beschränkt und kann auch die Pflicht zur Registrierung von Nutzern, zur Verschlüsselung des Zugangs mit einem Passwort oder – im äußersten Fall – zur vollständigen Sperrung des Zugangs umfassen.“

Mit dem Dritten Gesetz zur Änderung des TMG wurde die Störerhaftung für Betreiber öffentlicher WLANs abgeschafft. Die für Rechteinhaber bestehende Möglichkeit, die Sperrung einzelner Internetseiten zu verlangen, wurde durch das Urteil des BGH jedoch wesentlich weiter ausgelegt und könnte damit wieder für neue Unsicherheiten sorgen.

5.5 Rundfunk-Staatsverträge

Mit dem 21. Rundfunkänderungsstaatsvertrag (RÄStV) wurden der Rundfunkstaatsvertrag (RStV), der Rundfunkbeitragsstaatsvertrag, der ZDF-Staatsvertrag sowie der Deutschlandradio-Staatsvertrag an die ab 25. Mai 2018 in Deutschland unmittelbar geltende europäische Datenschutz-Grundverordnung (DS-GVO) angepasst (GVBl. LSA 2018, S. 22). Ziel war dabei der Erhalt des sog. Medienprivilegs.

Bisher regelten in diesem Bereich verschiedene nationale Vorschriften (z. B. § 41 BDSG, § 57 RStV) die beschränkte Anwendbarkeit von Datenschutzrecht und Datenschutzaufsicht auf Medien und Presse. Dieses sog. Medienprivileg ist Ausfluss der Medien- und Pressefreiheit des Art. 5 Abs. 1 GG.

Die DS-GVO selbst sieht kein Medienprivileg vor, jedoch werden die Mitgliedstaaten mit Blick auf das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie die Medienfreiheit gemäß Art. 85 Abs. 1 DS-GVO zum Erlass von Regelungen über Abweichungen oder Ausnahmen von der DS-GVO verpflichtet, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit den zuvor genannten Rechten in Einklang zu bringen. Aus Art. 85 Abs. 2 DS-GVO folgt, dass Ausnahmen und Abweichungen nur im Rahmen der genau bezeichneten Kapitel der DS-GVO möglich sind und jeweils erforderlich sein müssen, um die kollidierenden Grundrechte in Einklang zu bringen.

Keines der genannten Rechte und keine der Grundfreiheiten genießen im Rahmen von Art. 85 DS-GVO einen Vorrang. Die Verpflichtung, mittels Abweichungen und Ausnahmen von bestimmten Vorschriften der DS-GVO den Schutz personenbezogener Daten und konkurrierender Rechte und Freiheiten in Einklang zu bringen, setzt in jedem Fall eine Abwägung voraus („soweit dies erforderlich ist“). Ein pauschaler undifferenzierter Ausschluss der Anwendung sämtlicher Vorschriften der in Art. 85 Abs. 2 genannten Kapitel der DS-GVO würde gegen EU-rechtliche Vorgaben verstoßen.

Genau das war allerdings bei den Entwürfen für die Novellierung der Rundfunk-Staatsverträge der Fall. Hier wurden pauschal die Anwendbarkeit eines Großteils der Vorschriften der Datenschutz-Grundverordnung für den journalistischen Bereich ausgeschlossen und lediglich drei Artikel für anwendbar erklärt. Dadurch wurde nach Auffassung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder das durch Art. 85 DS-GVO vorgegebene Regel-Ausnahme-Verhältnis ins Gegenteil verkehrt. Mit einer Entschließung vom November 2017 wurden diese Forderungen für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen zur Umsetzung der DS-GVO im Medienrecht bekräftigt (**Anlage 18**).

Auch bei den Beratungen zur Änderung des MDR-Staatsvertrages äußerten die Landesdatenschutzbeauftragten von Sachsen-Anhalt, Sachsen und Thüringen Kritik am

vorliegenden Entwurf, zumal dieser inhaltlich mit den im 21. RÄStV vorgesehenen Regelungen übereinstimmte. Allerdings stand der 21. RÄStV zu diesem Zeitpunkt schon kurz vor der Unterzeichnung durch die Ministerpräsidenten der Bundesländer, sodass die Kritik zwar zur Kenntnis genommen, an den Regelungen des Entwurfs jedoch festgehalten wurde.

Der MDR-Staatsvertrag wurde von den Ministerpräsidenten der Länder Sachsen-Anhalt, Sachsen und Thüringen im Februar 2018 unterzeichnet und danach durch die jeweiligen Landesparlamente ratifiziert (GVBl. LSA 2018. S. 52). Der Landesbeauftragte wurde durch den Landtag Sachsen-Anhalt nicht mehr beteiligt.

Trotz der Vorgaben aus Art. 85 DS-GVO, Regelungen über Abweichungen oder Ausnahmen von bestimmten Kapiteln der DS-GVO zu treffen, falls dies erforderlich ist, um das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie die Medienfreiheit mit dem Recht auf Schutz der personenbezogenen Daten in Einklang zu bringen, wurde vom Gesetzgeber pauschal die Anwendbarkeit eines Großteils der Vorschriften der DS-GVO für den journalistischen Bereich ausgeschlossen. Damit wurde das Medienprivileg über den Schutz personenbezogener Daten gestellt.

5.6 Soziale Netzwerke

5.6.1 Verantwortlichkeit für Fanpages bei Facebook

Auch in seinem XII. Tätigkeitsbericht (Nr. 5.8.1) hatte der Landesbeauftragte über den Stand im Verfahren des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) gegen die Wirtschaftsakademie Schleswig-Holstein informiert, in dem es um die Beanstandung des Betriebs einer Facebook-Fanpage geht.

Nachdem das ULD sowohl vor dem Verwaltungsgericht Schleswig (9. Oktober 2013 – 8 A 14/12) als auch vor dem Oberverwaltungsgericht Schleswig-Holstein (4. September 2014 – 4 LB 20/13) gescheitert war, ging es in Revision und reichte im Januar 2015 eine Revisionsbegründung vor dem Bundesverwaltungsgericht ein. Dieses legte dem Europäischen Gerichtshof (EuGH) am 25. Februar 2016 sechs relevante Fragen zur Vorabentscheidung vor (Az.: 1 C 28/14). Neben der Frage, wer für die Datenverarbeitung im Rahmen von Fanpages verantwortlich ist, sollte der EuGH auch darüber entscheiden, ob deutsche Aufsichtsbehörden überhaupt für die Überprüfung und Kontrolle von Facebook zuständig sind und deutsches Datenschutzrecht anwendbar ist, da sich die Europazentrale von Facebook in Irland befindet und die deutsche Niederlassung von Facebook nur für Marketingmaßnahmen zuständig ist.

Nach der mündlichen Verhandlung am 27. Juni 2017 hat der Generalanwalt am 24. Oktober 2017 seine Schlussanträge vorgelegt (Az.: C-210/16). Darin empfiehlt er, Facebook Ireland und Facebook Inc. (USA) als gemeinsam Verantwortliche für die Datenverarbeitung anzusehen. Für die Datenverarbeitung im Rahmen der Fanpage, insbesondere das Tracking von Besuchern, soll nach Ansicht des Generalanwalts zudem der Betreiber der Fanpage gemeinsam mit Facebook Irland und USA verantwortlich sein. Dieser ermögliche schließlich durch die Einrichtung der Fanpage, dass die Aktivitäten seiner Seitenbesucher von Facebook ausgewertet werden können. Auch wenn der Fanpage-Betreiber nur auf anonyme Besucherstatistiken zugreifen

könne, mache er sich dennoch die Infrastruktur von Facebook zunutze und akzeptiere die Vertragsbedingungen. Er habe bestimmenden Einfluss auf die Verarbeitung und könne diese auch beenden, indem er die Fanpage schließe. Daher müsse er auch die Verantwortung für den Schutz personenbezogener Daten übernehmen.

Der Generalanwalt bejahte die Zuständigkeit der deutschen Aufsichtsbehörde für die Überprüfung der Datenverarbeitung von Facebook und die Anwendbarkeit deutschen Datenschutzrechts. Dies begründete er damit, dass die deutsche Niederlassung von Facebook die durch Facebook Ireland erhobenen Daten deutscher Nutzer auch gezielt für ihre Marketingaktivitäten in Deutschland nutzt.

Der EuGH folgte in seinem Urteil vom 5. Juni 2018 (C-210/16) im Wesentlichen den Schlussanträgen des Generalanwalts und stellte fest, dass der Betreiber einer Facebook-Fanpage gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich ist. Außerdem kann die Datenschutzbehörde des Mitgliedstaats, in dem dieser Betreiber seinen Sitz hat, sowohl gegen ihn als auch gegen die in diesem Mitgliedstaat niedergelassene Tochtergesellschaft von Facebook vorgehen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßten das Urteil des EuGH, das ihre langjährige Rechtsauffassung bestätigte und stellten in ihrer Entschließung vom Juni 2018 „Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern“ fest, dass für die Betreiber von Fanpages und für Facebook nunmehr dringender Handlungsbedarf besteht (**Anlage 21**).

Der Landesbeauftragte hat den Landes- und Kommunalbehörden empfohlen, auf einen Auftritt bei Facebook einstweilen zu verzichten bzw. eine vorhandene Präsenz zu deaktivieren. Zumindest ist eine Anpassung der Datenschutzhinweise unumgänglich. Die Staatskanzlei als Verantwortliche für das Landesportal hat nach entsprechenden Maßgaben des Landesbeauftragten die Datenschutzhinweise des Landesportals und der Fanpage bei Facebook geändert. Einer Überprüfung bedarf auch der Leitfaden zu den Social-Media-Aktivitäten der Landesverwaltung von 2016.

Nach dem Urteil des EuGH besteht natürlich auch für die Betreiber aus dem nichtöffentlichen Bereich Handlungsbedarf. Der Landesbeauftragte hat verantwortliche Stellen im Bereich von Unternehmen und Vereinen entsprechend beraten und sensibilisiert. Facebook selbst muss inhaltliche Angaben für eine Vereinbarung mit den Seitenbetreibern gem. Art. 26 DS-GVO liefern. Hierauf müssen die Seitenbetreiber entsprechend hinwirken.

5.6.2 Nutzung des „Gefällt-Mir“-Buttons

Wie sog. Social Plugins wie der „Gefällt-Mir“-Button von Facebook datenschutzkonform genutzt werden können, hatte der Landesbeauftragte bereits in seinem XII. Tätigkeitsbericht (Nr. 5.8.2) erläutert.

Da bei der direkten Einbindung des „Gefällt-Mir-Buttons“ schon beim Aufruf der Seite Nutzerdaten an Facebook übermittelt werden, empfahl der Landesbeauftragte z. B. die Verwendung der 2-Klick-Lösung, bei der eine Datenübermittlung erst erfolgt, wenn der Nutzer das Plugin aktiviert. Mittlerweile gibt es mit dem „Shariff“ eine nut-

zerfreundliche Weiterentwicklung, bei der die Aktivierung des Plugins entfällt und somit nur noch ein Klick erforderlich ist.

Dazu hatte das Landgericht Düsseldorf in seinem Urteil vom 9. März 2016 (AZ: 12 O 151/15) entschieden, dass die bloße Einbindung des „Gefällt-Mir“-Buttons von Facebook auf Webseiten ohne die Einwilligung der betroffenen Seitenbesucher und ohne Angabe über Zweck und Funktionsweise des Buttons gegen das Datenschutzrecht verstößt und damit wettbewerbswidrig ist. Da die Nutzer der Webseite nicht auf die Übermittlung ihrer Nutzerdaten in die USA hingewiesen wurden, stufte das Landgericht Düsseldorf die Einbindung des „Gefällt-Mir“-Buttons als unlauter im Sinne des § 3a Gesetz gegen den unlauteren Wettbewerb i. V. m. § 13 Telemediengesetz ein.

Das beklagte Unternehmen hatte gegen die Entscheidung Berufung eingelegt. Als Berufungsinstanz hat das Oberlandesgericht Düsseldorf den Prozess mit Beschluss vom 19. Januar 2017 (Az.: I-20 U 40/16) bis auf weiteres ausgesetzt und dem Europäischen Gerichtshof insgesamt sechs datenschutzrechtlich relevante Fragen zur Vorabentscheidung vorgelegt. Unter anderem soll geklärt werden, ob derjenige, der den „Gefällt-Mir“-Button von Facebook auf seiner Webseite einbindet, nach europäischem Recht datenschutzrechtlich verantwortlich ist, auch wenn er selbst den Datenverarbeitungsvorgang nicht beeinflussen kann. Hier dürfte wie bei den Fanpages (s. Nr. 5.6.1) das Prinzip der Mitverantwortung greifen.

5.6.3 Facebook – Weitere Dauerprobleme

Bereits in seinem XII. Tätigkeitsbericht (Nr. 5.8.1) berichtete der Landesbeauftragte über eine Anordnung, die der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit gegenüber der Facebook Ireland Ltd. erlassen hat. Mit dieser Anordnung wurde Facebook verpflichtet, die pseudonyme Nutzung seines Dienstes zuzulassen und die Sperrung eines Nutzerkontos, die aufgrund der pseudonymen Nutzung vorgenommen wurde, aufzuheben. Es wurde außerdem festgestellt, dass die Forderung der Vorlage amtlicher Lichtbildausweise (Personalausweis oder Reisepass) zum Identitätsnachweis durch Übersendung digitaler Kopien unzulässig ist.

Hiergegen setzte sich Facebook gerichtlich zur Wehr, woraufhin das Verwaltungsgericht Hamburg in einem Verfahren des vorläufigen Rechtsschutzes entschied, dass der Bescheid des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit einstweilen nicht vollzogen werden darf (VG Hamburg, Beschluss vom 3. März 2016, Az.: 15 E 4482/15). Da das Gericht im Rahmen des Eilverfahrens die Anwendbarkeit des deutschen Datenschutzrechts infrage gestellt hatte und mehr oder weniger den diesbezüglichen Argumenten von Facebook gefolgt war, erhob der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Beschwerde beim Oberverwaltungsgericht Hamburg.

Mit Beschluss vom 29. Juni 2016 (Az.: 5 Bs 40/16) entschied das Oberverwaltungsgericht Hamburg über die Beschwerde und wies diese zurück. Die Anordnung gegenüber Facebook durfte somit nicht vollzogen werden. Die Richter begründeten ihre Entscheidung im Wesentlichen mit der Rechtsunklarheit hinsichtlich der Zuständigkeit der Behörde bzw. Anwendbarkeit des Rechts innerhalb von Europa.

Nach dem damaligen Stand der Rechtsprechung des Europäischen Gerichtshofs (EuGH) war nicht geklärt, ob die EU-Datenschutzrichtlinie es erlaubt, dass der Datenschutzbeauftragte aufgrund nationaler Regelungen gegen die in Irland ansässige Antragstellerin mit hoheitlichen Mitteln vorgehen darf. Mittlerweile hat der EuGH in seinem Urteil vom 5. Juni 2018 (C-210/16) zur Verantwortlichkeit von Betreibern einer Facebook-Fanpage jedoch auch festgestellt, dass die Datenschutzbehörde des Mitgliedstaats, in dem dieser Betreiber seinen Sitz hat, sowohl gegen ihn als auch gegen die in diesem Mitgliedstaat niedergelassene Tochtergesellschaft von Facebook vorgehen darf (siehe Nr. 5.6.1).

In einem weiteren Urteil entschied das Landgericht Berlin am 16. Januar 2018 (16 O 341/15), dass Facebook mit seinen Voreinstellungen und Teilen seiner Nutzungs- und Datenschutzbestimmungen gegen deutsches Datenschutzrecht verstoße. So fordere u. a. das Telemediengesetz die Anbieter von Online-Diensten auf, die Nutzung anonym oder pseudonym zu ermöglichen. Dagegen verstoße die Klarnamenpflicht. Das Urteil ist jedoch noch nicht rechtskräftig, sondern wird in der nächsten Instanz beim Kammergericht Berlin verhandelt werden.

Im März 2018 wurde bekannt, dass von November 2013 bis Mai 2015 mit Hilfe einer App Daten von ca. 87 Millionen Facebook-Nutzern weltweit erhoben und an das Datenanalyseunternehmen Cambridge Analytica weitergeben wurden. Dieses hatte die Daten offenbar auch zur Profilbildung für politische Zwecke verwendet. Das Problem dabei war, dass die App durch einen Fehler nicht nur Zugriff auf die Daten der etwa 270.000 Facebook-Nutzer hatte, die darin eingewilligt hatten, sondern auch auf deren Freunde und die Freunde der Freunde.

Diesen Datenskandal nahm die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zum Anlass, im April 2018 eine Entschließung zu verabschieden, in der sie weitreichende Konsequenzen für Betreiber sozialer Netzwerke und insbesondere für Facebook fordert (**Anlage 19**). Zudem hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen.

Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzer betreffen.

5.7 WhatsApp-Nutzung – Weitergabe von Kontaktdaten

Bereits in seinem XII. Tätigkeitsbericht (Nr. 5.10) hatte der Landesbeauftragte über die Risiken beim Einsatz von WhatsApp berichtet. Dabei wurde vor allem auf die Nutzungsbedingungen verwiesen, in die der Nutzer einwilligen muss und mit denen er umfangreiche Rechte an der Kommunikation an WhatsApp abtritt. Auch die automatisierte Übertragung der Kontakte aus dem Adressbuch des Nutzers wurde kritisiert.

Zwar werden die übertragenen Nachrichten mittlerweile standardmäßig über eine Ende-zu-Ende-Verschlüsselung geschützt, die Metadaten – also wer hat wann mit

wem kommuniziert – werden jedoch weiterhin im Klartext übermittelt und können von WhatsApp für eigene Zwecke ausgewertet werden.

Dazu hat das Amtsgericht Bad Hersfeld in einem Sorgerechtsstreit, in dem es auch um die Smartphone-Nutzung eines elf Jahre alten Jungen ging, bezüglich der Übertragung der Kontaktdaten aus dem Adressbuch des WhatsApp-Nutzers folgendes festgestellt (Beschluss vom 20. März 2017, Az.: F 111/17 EASO):

„Wer den Messenger-Dienst "WhatsApp" nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen. Wer durch seine Nutzung von "WhatsApp" diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.“

Zwar gibt es auch technische Lösungen, die den Zugriff der App auf die Kontaktdaten verhindern können, jedoch ist aus Sicht des Landesbeauftragten die automatische Übertragung der Kontaktdaten an WhatsApp nur ein datenschutzrechtliches Problem von vielen. Zum einen gibt es nach wie vor Bestrebungen von Facebook, auf Nutzerdaten von WhatsApp zuzugreifen. Zum anderen ist WhatsApp nicht quelloffen, sodass nicht ausgeschlossen werden kann, dass die Verschlüsselung der Kommunikationsinhalte auf andere Weise wieder aufgehoben werden könnte. Außerdem werden die Metadaten unverschlüsselt gespeichert und können so zur Auswertung von Kommunikationsbeziehungen genutzt werden. In diesem Zusammenhang ist auch fraglich, ob die Zustimmung des Nutzers zu den Nutzungsbedingungen und der Datenschutzrichtlinie durch Installation der App die Anforderungen an eine Einwilligung gem. Art. 7 DS-GVO erfüllt.

Aus den genannten Gründen begegnet die Nutzung von WhatsApp durch Unternehmen und Behörden nach wie vor erheblichen datenschutzrechtlichen Bedenken. Für geschlossene Benutzergruppen empfiehlt es sich, die Nutzung alternativer Messenger-Dienste zu prüfen.

5.8 Digitaler Nachlass

Mit der zunehmenden Digitalisierung der Gesellschaft stellen Daten einen immer größeren Bestandteil des Nachlasses dar. Beim sog. „Digitalen Nachlass“ handelt es sich meist um Inhalte in sozialen Netzwerke wie Facebook, Instagram oder Snapchat, in E-Mail-Konten, in Cloud-Speichern, bei Streamingdiensten, Spieleportalen oder sonstigen Internetdiensten wie z. B. Amazon oder eBay, die von der verstorbenen Person zu Lebzeiten angelegt bzw. eingerichtet wurden. Auf Servern vieler dieser Internet-Diensteanbieter können das gespeicherte E-Mails, in einer Cloud abgelegte Dokumente oder in sozialen Netzwerken gespeicherte Fotos und mit Freunden geteilte Inhalte sein.

Wenn Passwörter und andere Zugangsdaten von Nutzerkonten zu Internetdiensten oder Profilen den Hinterbliebenen nicht vorliegen, erschwert das die rechtzeitige Abwicklung durch diese oder macht sie sogar unmöglich. Umfragen bestätigen, dass

sich nur sehr wenige Internetnutzer mit diesem Thema beschäftigen und entsprechende Vorsorge hinsichtlich ihres „Digitalen Nachlasses“ treffen. Oft sind Online-Aktivitäten auch mit laufenden, kostenpflichtigen Verträgen verbunden und solange die Diensteanbieter nichts vom Tod des Nutzers erfahren, laufen diese Verträge weiter.

Wie bei jeder gesellschaftlichen Entwicklung führt auch das Thema „Digitaler Nachlass“ zu kontroversen juristischen Diskussionen, denn die meisten Erben möchten auf diesen Nachlass ebenso zugreifen können wie auf herkömmliche Briefe und Papierunterlagen, die sie im Todesfall von ihren Angehörigen erben.

Weitgehende Einigkeit besteht darüber, dass gemäß § 1922 BGB alle Daten – sowohl geschäftlicher als auch intimer Natur – auf die Erben übergehen. Ebenso besteht Einigkeit darüber, dass die Rechtsnachfolge von Todes wegen durch Allgemeine Geschäftsbedingungen der Provider nicht ausgeschlossen werden kann. Dies wäre ein Verstoß gegen § 307 BGB.

Umstritten war allerdings die Frage, ob das in § 88 Telekommunikationsgesetz (TKG) geregelte Fernmeldegeheimnis einem Zugriff der Erben auf die Daten des Erblassers entgegensteht. In einem aktuellen Fall forderten die Eltern von Facebook den Zugang zum Konto ihrer verstorbenen Tochter. Facebook lehnte dies mit Verweis auf das Fernmeldegeheimnis (§ 88 Abs. 3 TKG) bzw. die mitumfassten Daten Dritter ab. Nunmehr hat der Bundesgerichtshof hierzu am 12. Juli 2018 in letzter Instanz mit einem Grundsatzurteil Rechtsklarheit geschaffen (BGH III ZR 183/17). Der Vertrag über ein Nutzerkonto bei einem sozialen Netzwerk geht grundsätzlich im Wege der Gesamtrechtsfolge auf die Erben des ursprünglichen Kontoberechtigten über. Erben haben damit gegenüber einem Netzwerkbetreiber Anspruch auf Zugang zu diesem Konto, einschließlich der darin gespeicherten Kommunikationsinhalte.

5.9 Bewertungsportale

Zu Bewertungsportalen hatte der Landesbeauftragte bereits im XII. Tätigkeitsbericht (Nr. 5.13) umfassende Hinweise gegeben. Er beobachtet die Entwicklung in Gestalt von vielfältiger Rechtsprechung weiter.

Das Oberlandesgericht Frankfurt hat unter Verweis auf die Rechtsprechung des Bundesverfassungsgerichts entschieden, dass eine Äußerung, in der sich Tatsachen und Meinungen vermengen, die jedoch unter Berücksichtigung des Gesamtkontextes maßgebend durch die Elemente der Stellungnahme, des Dafürhaltens oder Meinens geprägt ist, insgesamt als Werturteil bzw. Meinungsäußerung (Art. 5 Abs. 1 GG) einzuordnen ist und als solche von dem Grundrechtsschutz der Meinungsfreiheit erfasst wird (OLG Frankfurt, Beschluss vom 18. Juni 2015, 16 W 29/15, m. w. N., juris). Der Fall betraf folgende Äußerung: „Eine solche Behandlung schadet und gefährdet nicht nur den Einzelnen, das Vertrauen in den Berufsstand der gesamten Ärzteschaft wird untergraben“.

Nach der Rechtsprechung des Bundesverfassungsgerichts muss die Behauptung wahrer Tatsachen, die Vorgänge aus der Sozialsphäre betreffen, grundsätzlich hingenommen werden, denn das Persönlichkeitsrecht verleiht keinen Anspruch darauf, nur so in der Öffentlichkeit dargestellt zu werden, wie es genehm ist. Zu den hinzunehmenden Folgen der eigenen Entscheidungen und Verhaltensweisen gehören

auch solche Beeinträchtigungen, die sich aus nachteiligen Reaktionen Dritter auf die Offenlegung wahrer Tatsachen ergeben, solange sie sich im Rahmen der üblichen Grenzen individueller Entfaltungschancen halten. Die Schwelle zur Persönlichkeitsrechtsverletzung wird bei der Mitteilung wahrer Tatsachen über die Sozialsphäre regelmäßig erst überschritten, wo sie einen Persönlichkeitsschaden befürchten lässt, der außer Verhältnis zu dem Interesse an der Verbreitung der Wahrheit steht (BVerfG, Beschluss vom 29. Juni 2016, 1 BvR 3487/14[5], bezüglich Äußerungen die schleppende Zahlungsmoral einer Firma betreffend).

Ein Urteil des OVG Münster vom 19. Oktober 2017 (16 A 770/17) befasste sich mit der Möglichkeit, in einem Bewertungsportal zu Kfz-Kennzeichen Fahrverhalten zu bewerten. Autofahren findet danach zwar in der Sozialsphäre statt, der Kontakt zu anderen Verkehrsteilnehmern ist jedoch Begleiterscheinung, nicht aber beabsichtigt. Eine Prangerwirkung ist daher nicht zuzumuten, insbesondere da auf Nutzerseite zweckwidrige Motive oder unrichtige Bewertungen nicht fernliegend sind. Auch können Halter und Fahrer auseinanderfallen. Die Lesbarkeit für die Öffentlichkeit war daher zu Recht untersagt worden.

In einer weiteren Entscheidung zu Arztbewertungsportalen vom 20. Februar 2018 (Az.: VI ZR 30/17) hat der Bundesgerichtshof einer Ärztin bezüglich ihres Profils einen Löschungsanspruch gewährt. Das Portal hatte, da sie nicht bereit war, monatliche Zahlungen zu leisten, neben der Bewertung Hinweise auf andere Ärzte gleicher Fachrichtung platziert. Damit habe das Portal die Rolle als neutraler Informationsmittler verlassen, das Interesse der Ärztin trete damit nicht hinter das Informationsinteresse zurück.

6 Öffentliche Sicherheit, Meldewesen

6.1 Novellierung des BKAG

Die erfolgte Novellierung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft sowohl die Polizeibehörden des Bundes als auch die Polizeibehörden der Länder. Letzteres ist auch der Grund, weshalb sich der Landesbeauftragte mit dem BKAG beschäftigt.

Ausgangspunkt der Novellierung war die Umsetzung des Urteils des Bundesverfassungsgerichts zum BKAG vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/09) sowie der neuen EU-Richtlinie 2016/680 für den Datenschutz im Bereich Justiz und Inneres (JI-Richtlinie) vom 27. April 2016. Der Gesetzgeber hat sich jedoch nicht darauf beschränkt, diese Maßgaben umzusetzen. Er hat darüber hinaus einen neuen, relativ undifferenzierten Informationspool geschaffen und wesentlich längere Speicherfristen für Daten ermöglicht. Viele der datenschutzrechtlichen Anforderungen an ein modernes polizeiliches Datenschutzrecht berücksichtigte er allerdings nicht.

Mit der Novellierung werden die bisherigen Verbunddateien des bundesweiten INPOL-Systems abgeschafft und durch einen Informationspool ersetzt. Die bisherige

[5] https://www.bverfg.de/e/rk20160629_1bvr348714.html

Differenzierung nach verschiedenen Dateien – und damit auch verschiedenen Zwecken – gibt es seit dem 25. Mai 2018 nicht mehr. Durch die neue Struktur werden die gespeicherten Daten nicht mehr einzelnen Dateien zugeordnet. In der Folge gibt es keine spezifischen Vorgaben mehr zum Zweck der jeweiligen Speicherung, zu Aussonderungsprüffristen und zu den weiteren bislang in den jeweiligen Errichtungsanordnungen vorgesehenen Verfahrenssicherungen.

Die Veränderung ist so grundlegend, dass die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) anlässlich ihrer Tagung im März 2017 eine Entschließung „Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte“ (**Anlage 13**) gefasst hat. Die DSK lehnt insbesondere den Verzicht auf Errichtungsanordnungen ab. Diese waren bislang Ausgangspunkt datenschutzrechtlicher Kontrollen. Sie dienten aber vor allem auch als Mittel der Selbstkontrolle für die Polizeibehörden. In den Errichtungsanordnungen ist insbesondere festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Diese Bindung an einen bestimmten Zweck ist eine wesentliche verfassungsrechtliche Vorgabe für die Speicherung. Die neuen Regelungen führen sowohl zu umfassenden übergreifenden Verknüpfungen der polizeilichen Aufgaben bzw. Phänomenbereiche von Kriminalität als auch zu Abgleichen aller gespeicherten Personen. Sie lösen die Zweckbindung in Teilen auf und verkürzen die Kontrollmöglichkeiten der Datenschutzbehörden von Bund und Ländern.

Die Novellierung des BKAG ist zwischenzeitlich abgeschlossen. Es trat in der Fassung vom 1. Juni 2017 (BGBl I S. 1354, 1392) am 25. Mai 2018 in Kraft, auch wenn nach wie vor datenschutzrechtliche Bedenken gegen verschiedene Regelungen bestehen. Die Bundesländer – und damit auch Sachsen-Anhalt – werden sich an den neuen Regelungen des BKAG orientieren, wenn sie ihre Polizeigesetze überarbeiten. Für Sachsen-Anhalt wird der Landesbeauftragte datenschutzrechtliche Aspekte und Kritikpunkte zu Rechtsetzungsvorhaben bezogen auf das Polizeirecht weiterhin geltend machen. Der schlichte Verweis, es gäbe gleiche Regelungen im BKAG, wird als Begründung für entsprechende Landesregelungen nicht ausreichen.

Da die mit der Novellierung des BKAG getroffenen Regelungen in Teilen – z. B. Auflösung zweckgebundener Dateien zugunsten von unspezifizierten Datensammlungen – datenschutzrechtlich durchaus problematisch sind, sollte das Gesetz nicht ohne Weiteres als Blaupause für das SOG LSA genutzt werden.

6.2 SOG LSA

In seinem XII. Tätigkeitsbericht (Nr. 6.1) hat sich der Landesbeauftragte zum Vierten und Fünften Änderungsgesetz zum Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) geäußert. Gegenstand der Änderungen des SOG LSA war die Erweiterung der Möglichkeiten zur Telekommunikationsüberwachung und deren spätere Anpassung – sprich Eingrenzung – nach den Vorgaben, die das Landesverfassungsgericht im Normenkontrollverfahren (LVG 9/13, NVwZ 2015, 438) gemacht hat.

Mit dem Sechsten Änderungsgesetz zum SOG LSA vom 12. Juli 2017 (GVBl. LSA S. 130) wurde die sog. Body-Cam als Modellprojekt bis Juni 2019 im öffentlichen Verkehrsraum der kreisfreien Städte des Landes und die Kennzeichnungspflicht für

Polizeibeamte eingeführt. Soweit es die Kennzeichnungspflicht betrifft, hat der Landesbeauftragte im Ergebnis keine datenschutzrechtlichen Bedenken mehr erhoben. Was den Einsatz der Body-Cam anbelangt, wurden bis zuletzt wesentliche datenschutzrechtliche Erwägungen nicht berücksichtigt.

Im Wesentlichen blieben Fragen zum Zweck und zur Eignung der Maßnahme, zur Datenerhebung im Vorfeld von Gefahrensituationen im Sinne einer Vorratsdatenspeicherung, zur Bestimmtheit der Regelung, zur Ausweitung der Datenerhebung auf Tonaufzeichnungen und damit zum Kernbereichsschutz, zur Erfassung unbeteiligter Dritter, zur Versammlungsfreiheit und zum Umgang mit Amts- und Berufsgeheimnisträgern offen. Die Auswertung des Modellprojektes wird auch zeigen, inwieweit die Body-Cam den hohen Erwartungen an ihren Einsatz gerecht werden kann (vgl. zu ersten Praxiserfahrungen LT-Drs. 7/3203).

Kernpunkte des Entwurfes eines Siebten Änderungsgesetzes zum SOG LSA (LT-Drs. 7/2402) sind die Einführung des Begriffes der „terroristischen Straftat“ sowie die Schaffung von Rechtsgrundlagen für Meldeauflagen, Aufenthaltsanordnungen, Kontaktverbote und die elektronische Aufenthaltsüberwachung für terroristische Gefährder. Der Landesbeauftragte hat sich in seiner Stellungnahme zum Entwurf gegenüber dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt kritisch zu den geplanten Regelungen zur „terroristischen Straftat“, zur Meldeauflage und zur elektronischen Fußfessel geäußert. Die Maßnahmen erscheinen insgesamt ungeeignet zur Abwehr terroristischer Anschläge. Der Gesetzentwurf der Landesregierung wurde im März 2018 in den Landtag von Sachsen-Anhalt eingebracht. Die Beratungen in den Ausschüssen dauern an. Der Landesbeauftragte hat seine fortbestehenden Bedenken in einer Stellungnahme gegenüber dem Ausschuss für Inneres und Sport vorgetragen.

Mit Artikel 3 des Entwurfs des „Gesetzes 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“ (LT-Drs. 7/3207) soll das SOG LSA nochmals und grundlegend geändert werden. Anpassungen an die europäische Datenschutzrechtslage sind dabei zwingend, weil die Richtlinie (EU) 2016/680 einer Umsetzung in nationales Recht bedarf. Die Anpassungen im SOG LSA beschränken sich allerdings nicht auf das aus datenschutzrechtlicher Sicht Notwendige. Vielmehr wird der Versuch unternommen, Regelungen aus dem BKA-Recht in das Landespolizeirecht zu übertragen. Wegen der Einzelheiten wird auf die Ausführungen in den Nrn. 1.3 und 6.1 dieses Tätigkeitsberichtes verwiesen. Der Landesbeauftragte wird das Gesetzgebungsverfahren auch im Rahmen der parlamentarischen Beratungen weiter begleiten.

Die im Gesetzentwurf vorgesehenen Regelungen zu Zuverlässigkeitsüberprüfungen entsprechen in ihrer derzeitigen Entwurfsfassung noch nicht den datenschutzrechtlichen Anforderungen. Mit ihrer Entschließung vom April 2018 „Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren“ (**Anlage 20**) hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder den Rahmen für entsprechende Regelungen aufgezeigt.

Das SOG LSA unterlag im Berichtszeitraum wiederholten Änderungen, bei denen trotz entsprechender Stellungnahmen des Landesbeauftragten den berechtigten verfassungs-/datenschutzrechtlichen Maßgaben nicht ausreichend Rechnung getragen wurde. Auch für die nahe Zukunft sind erneute Änderungen absehbar. Der Landesbeauftragte wird bei jeder Änderung weiterhin darauf dringen, dem Datenschutz angemessene Geltung zu verschaffen.

6.3 Kontrolle der Falldatei Rauschgift

Die bundesweite Falldatei Rauschgift (FDR) gibt es seit über 30 Jahren. Die FDR dient der Polizei zur umfassenden Rauschgift-Lagebilddarstellung und ermöglicht den beteiligten Behörden, belastbare Statistiken und Analysen zu erstellen. In Einzelfällen soll aber auch der Rückgriff auf täterbezogene Auskünfte im Bereich der Betäubungsmittelkriminalität möglich sein. Inhalt und Umfang der in der FDR gespeicherten Daten waren in den 30 Jahren ihrer Existenz immer wieder Gegenstand von Diskussionen zwischen Polizei und Datenschutzbehörden. Im Kern geht es darum, dass ausschließlich Fälle mit erheblicher, länderübergreifender oder internationaler Bedeutung Aufnahme in die Datei finden sollen und dass – anders als in Arbeits- und Ermittlungsdateien – in die FDR zudem nur sog. gesicherte Daten einfließen.

Um zu prüfen, inwieweit der Datenbestand der FDR den gesetzlichen Vorgaben entspricht, hat der Arbeitskreis Sicherheit der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) eine gemeinsame Prüfung vereinbart und durchgeführt. Im Ergebnis musste festgestellt werden, dass auch Sachverhalte in die FDR eingestellt wurden, die den dafür festgelegten Kriterien nicht entsprechen. Es fanden sich zahlreiche Speicherungen, bei denen sich kein ausreichender Tatverdacht belegen ließ oder die eben gerade keinen erheblichen, länderübergreifenden oder internationalen Bezug hatten. Für die beim Landeskriminalamt Sachsen-Anhalt konkret geprüften Datensätze der FDR wurden jedoch keine unzulässigen Speicherungen konstatiert.

Die Ergebnisse nahm die DSK im November 2016 zum Anlass, die Entschließung „Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf“ (**Anlage 9**) zu fassen. Die DSK fordert darin nicht nur, die in der FDR festgestellten Mängel zu beheben. Sie verlangt darüber hinaus auch die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizeien. Erst recht sei dies vor dem Hintergrund der Übernahme von Daten aus der FDR in den allgemeinen Polizeilichen Informations- und Analyseverbund (PIAV) erforderlich.

Die mit der Entschließung vorgenommene Verallgemeinerung auf alle Verbunddateien der Polizeien ist zwingend geboten. Wie auch zuletzt die Vorkommnisse um den Entzug von Akkreditierungen beim G 20-Gipfel in Hamburg gezeigt haben, werden in polizeilichen Dateien immer wieder Daten vorgehalten, deren Speicherung von Beginn an nicht rechtmäßig war oder bei denen die Speicherung im Verlaufe der Zeit rechtswidrig wurde. Solche Daten dürfen nicht ungeprüft in andere Datenbestände überführt werden.

In polizeilichen Dateien werden große Mengen von personenbezogenen Daten der Bürgerinnen und Bürger gespeichert. Die Rechtmäßigkeit dieser Speicherungen ist durchaus nicht immer gegeben, was Prüfungen des Landesbeauftragten belegen. Insbesondere vor der Überführung von polizeilichen Datensätzen in PIAV bedarf es einer Überprüfung der Rechtmäßigkeit der Speicherung.

6.4 Kontrolle der Rechtsextremismusdatei

Die Kontrollverpflichtung, die der Landesbeauftragte in seinem XII. Tätigkeitsbericht (Nr. 8.3) bezogen auf die Antiterrordatei beschrieben hat, trifft ihn für die Rechtsextremismusdatei nach dem Gesetz über die Einrichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (RED-G) gleichermaßen.

Nach § 11 Abs. 2 RED-G ist die Durchführung des Datenschutzes durch den Landesbeauftragten mindestens alle zwei Jahre zu kontrollieren. Beteiligte Stellen des Landes Sachsen-Anhalt im Sinne einer Berechtigung zum Einstellen von Daten in die Rechtsextremismusdatei sind die Verfassungsschutzbehörde des Landes Sachsen-Anhalt und das Landeskriminalamt Sachsen-Anhalt. Sie tragen nach § 9 Abs. 1 RED-G die datenschutzrechtliche Verantwortung für die in der Rechtsextremismusdatei gespeicherten Daten.

Der Landesbeauftragte hat die nach RED-G erforderlichen Kontrollen bei der Verfassungsschutzbehörde des Landes Sachsen-Anhalt und beim Landeskriminalamt Sachsen-Anhalt im Jahre 2017 durchgeführt.

Bezogen auf die konkreten Gegenstände der Kontrollen konnte der Landesbeauftragte feststellen, dass die Speicherungen seitens der verantwortlichen Stellen datenschutzrechtlich nicht zu beanstanden waren.

6.5 Nutzung von Facebook durch das LKA

Aufgrund der Anfrage einer Bürgerin wurde der Landesbeauftragte darauf aufmerksam, dass das Landeskriminalamt Sachsen-Anhalt (LKA) eine Facebook-Seite betreibt. Durch das zuständige Ministerium für Inneres und Sport des Landes Sachsen-Anhalt (MI) bzw. das LKA war der Landesbeauftragte bis dahin nicht von der Facebook-Nutzung durch das LKA in Kenntnis gesetzt worden. Die Bürgerin fand es „toll“, dass das LKA nunmehr bei Facebook präsent ist. Sie führte weiter aus, dass Facebook-Nutzer durch das LKA aufgefordert worden seien, Bild- und Videomaterial zu einem Ermittlungsvorgang der Polizei auf Facebook hochzuladen. Und dann stellte die Bürgerin die entscheidenden Fragen:

„Kann ich davon ausgehen, dass Videos und Fotos, welche ich auf dieser Facebook-Polizei-Seite hochlade, ausschließlich dem LKA zur Verfügung gestellt werden und ausschließlich deutschem Recht unterliegen? Oder werden auch diese Bilder nach den Facebook-AGB oder -datenrichtlinien behandelt? Ich kann diesbezüglich keine ergänzenden Datenschutzhinweise auf der LKA-Seite finden. Wie ich gerade sehe, hat die Facebook-Nutzerin … gerade einen zustimmenden Kommentar auf der Facebook-Seite des LKA abgegeben. Wenn es sich bei dieser Facebook-Nutzerin um die ehemalige … des Innenministers handeln sollte, kann man wohl davon ausge-

hen, dass das Innenministerium die Facebook-Seite beauftragt hat. Dann sollte ja alles seine Richtigkeit haben und den deutschen Gesetzen unterliegen."

Es hatte nicht alles seine Richtigkeit und zustimmende Kommentare von Beschäftigten des Innenministers gewährleisten die Rechtmäßigkeit auch nicht.

Der Landesbeauftragte hat aufgrund der Anfrage das LKA zur Stellungnahme aufgefordert. In seiner ersten Stellungnahme hat das LKA seine Vorgehensweise als zulässig gerechtfertigt und sich dafür auf die Social-Media-Strategie des Landes Sachsen-Anhalt berufen. Da die in Bezug genommene Social-Media-Strategie dem Landesbeauftragten nicht bekannt war, bat er das LKA um Übersendung derselben. Zu seiner Überraschung war die Übersendung dann nicht möglich. Der Landesbeauftragte wurde an die Staatskanzlei und das Ministerium für Kultur des Landes Sachsen-Anhalt verwiesen. Auch dort bedurfte es zweier Anläufe, um die vollständigen Unterlagen übersendet zu bekommen. Einschlägig waren diese für das Vorgehen des LKA allerdings nicht.

Seine Rechtsauffassung hat der Landesbeauftragte dann dem LKA und dem MI als zuständiger Fachaufsicht mitgeteilt. Bei der Bewertung muss zunächst unterschieden werden, zu welchem Zweck das LKA seine Facebook-Seite nutzt. Zum einen kann eine Facebook-Seite zum Zwecke der Präsenz und Selbstdarstellung in sozialen Medien gedacht sein. Vorliegend hat das LKA die Facebook-Seite darüber hinaus zu Ermittlungszwecken genutzt.

Was den Betrieb der Facebook-Seite zum Zwecke der Präsenz in sozialen Medien betrifft, hat der Landesbeauftragte auf seine bereits wiederholt geäußerte Auffassung verwiesen, dass Facebook nicht datenschutzgerecht nutzbar sei. Das LKA ist als verantwortliche Stelle nach dem DSG LSA dafür mitverantwortlich, die Rechtmäßigkeit seines Handelns zu gewährleisten. Da für einmal auf Facebook eingestellte Daten keine Sachherrschaft mehr besteht, man vielmehr allein den intransparenten, sich fortwährend ändernden Regelungen des Netzwerkbetreibers unterliegt, ist die Nutzung von Facebook mit dem bestehenden Datenschutzrecht, zu dessen Einhaltung auch das LKA verpflichtet ist, nicht vereinbar (s. Nr. 5.6.1 mit Hinweisen zum Urteil des EuGH). Einer Überprüfung bedarf insofern auch der Entwurf der Rahmenkonzeption für eine Social Media-Strategie der Polizei des Landes, zu welcher der Landesbeauftragte das Ministerium für Inneres und Sport beraten hat.

Soweit es die Nutzung von Facebook in Ermittlungsverfahren betrifft, kommt hinzu, dass für derartige Ermittlungsmaßnahmen die Voraussetzungen nach der Strafprozessordnung (StPO) vorliegen müssen. Die insoweit seitens des LKA vorgetragenen Argumente konnten das Vorgehen nicht rechtfertigen. Der in Bezug genommene Erlass zu den „Richtlinien über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Strafverfahren" vom 22. Juni 2005 war nicht geeignet, die Maßnahme des LKA zu decken. Der Erlass sieht nämlich vor, Fahndungsaufrufe im Internet auf speziellen Seiten der Polizeibehörden zu bündeln. Private Internetdienstanbieter, insbesondere Web 2.0-Dienste und soziale Netzwerke, können zwar bei einer auch im Einzelfall schwerwiegenden Straftat zur besseren Verbreitung der Fahndung eingeschaltet werden, wenn andere Maßnahmen, die den Tatverdächtigen oder andere Betroffene weniger beeinträchtigen, erheblich weniger oder keinen Erfolg versprechen. Der Fahndungsaufruf hätte aber die Aufforderung

enthalten müssen, dass sachdienliche Hinweise unmittelbar (z. B. per Telefon oder E-Mail) an die Strafverfolgungsbehörden zu richten sind und eben nicht in das soziale Netzwerk oder auf Seiten privater Internetdienstanbieter eingestellt werden. Der Landesbeauftragte monierte dies zusammen mit weiteren Feststellungen.

Mit seiner erneuten Stellungnahme hat das LKA mitgeteilt, dass es die Nutzung der Facebook-Seite zu ermittlungstaktischen Zwecken eingestellt habe und nunmehr lediglich Informationen über die Behörde und deren Erreichbarkeiten abgebildet würden.

6.6 Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung

Die Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen werden auf dem Gebiet der polizeilichen Telekommunikationsüberwachung in Zukunft ein gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ) mit Sitz in Leipzig nutzen. Die beteiligten fünf Bundesländer haben das in einem „Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts“ (GKDZ-StV) vereinbart.

Über den Wortlaut des Staatsvertrages wurde länger diskutiert. Bereits Anfang 2015 wurden die Landesbeauftragten der beteiligten Länder zu ersten Informationsveranstaltungen beim federführenden Sächsischen Staatsministerium des Innern eingeladen. Diese und die weiteren Beratungen boten den Innenressorts und den Landesbeauftragten wiederholt die Gelegenheit zum Austausch. Trotz aller Beratung und Abstimmung fanden nicht alle datenschutzrechtlichen Belange angemessenen Eingang in den Vertragstext.

In seinen Stellungnahmen gegenüber dem Landtag von Sachsen-Anhalt und dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt hat der Landesbeauftragte auf nach wie vor ungeklärte Problemstellungen hingewiesen. Zu den wichtigsten gehört die Frage nach der Trennung der Daten der einzelnen Polizeien voneinander. Der Vertragstext erwähnt zwar diese Trennung. Welche Maßnahmen für die Trennung erforderlich sind, könne aber erst nach erfolgter Risiko- und Sicherheitsanalyse festgelegt werden. Diese ist dem Landesbeauftragten bisher allerdings nicht bekannt. Die Bestimmung von Rahmenbedingungen der Risikoanalyse und des Sicherheitskonzeptes durch die Trägerländer erst in der Satzung der Anstalt erscheint deshalb verspätet. Das Sicherheitskonzept müsste wesentliche Aspekte der Trennung von Daten regeln, auf die, da sie erst mit der Satzung geregelt werden sollen, durch die Datenschutzbeauftragten nur wesentlich erschwert noch Einfluss genommen werden kann.

Im GKDZ-StV war auch eine Regelung vorgesehen, die die Kontrollrechte der Landesbeauftragten unzulässig verkürzt hätte. Nach dem Vertragstext sollte es ausreichen, wenn der Sächsische Datenschutzbeauftragte die Landesbeauftragten der anderen beteiligten Länder zu Fragen in Bezug auf die Kernaufgabe – mithin die Telekommunikationsüberwachung – konsultiert. Das kann aber mit Blick darauf, dass die Polizei jedes beteiligten Bundeslandes für ihre Telekommunikationsüberwachungsmaßnahmen und die dadurch entstandenen Daten selbst rechtlich verantwortlich ist,

nicht richtig sein. Darauf hat der Landesbeauftragte gegenüber dem Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt ausdrücklich hingewiesen, woraufhin eine Änderung des Vertragstextes erreicht werden konnte (GVBl. LSA 2017, 226). Anders als im Thüringer Landtag kam eine Entschließung mit datenschutzrechtlichen Detailforderungen (LT-Drs. 7/1738) jedoch nicht zustande.

Auch wenn letztendlich nicht alle datenschutzrechtlichen Aspekte durch den Wortlaut des und die Begründung zum GKDZ-StV hinreichend beachtet wurden, hat der Landesbeauftragte im Rahmen seiner Beteiligung zum Entwurf eines Gesetzes zum GKDZ-StV auf datenschutzrechtliche Anmerkungen verzichtet. Der Wortlaut eines Staatsvertrages ist im Ratifizierungsverfahren nicht mehr änderbar.

Der GKDZ-StV klärt mit Wortlaut und Begründung nicht alle datenschutzrechtlichen Fragen, die derart eingriffsintensive Maßnahmen wie polizeiliche Telekommunikationsüberwachungen in einer gemeinsamen Einrichtung mit sich bringen. Es bedarf weiterer Abstimmungen zur Ausgestaltung von Satzung, Sicherheitskonzept, Risiko- und Sicherheitsanalyse. Kontrollen vor Ort wird es dann vorbehalten sein, die rechtmäßige Umsetzung der Überwachungsmaßnahmen zu prüfen.

6.7 Sicherheitsakten

In den vergangenen Tätigkeitsberichten (vgl. XII. Tätigkeitsbericht Nr. 6.6) hat der Landesbeauftragte regelmäßig über seine Kontrollen und deren Ergebnisse im Bereich des Geheimschutzes berichtet. Seit einigen Jahren hat es sich der Landesbeauftragte zur Aufgabe gemacht, das Führen von Sicherheitsakten regelmäßig zu kontrollieren. Dafür gibt es gute Gründe.

Sich einer Sicherheitsüberprüfung unterziehen zu lassen, suchen sich die Betroffenen nicht aus. Es gibt Aufgaben, die erfordern solch eine Überprüfung, um im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse vor der Kenntnisnahme durch Unbefugte zu schützen und den Zugang von Personen zu verhindern, bei denen ein Sicherheitsrisiko nicht ausgeschlossen werden kann. Das nennt man personeller Geheimschutz, und es ist nur ein Aspekt des Geheimschutzes. Unter datenschutzrechtlichen Gesichtspunkten ist es aber ein wesentlicher Aspekt, weil er die Sicherheitsüberprüfung der Betroffenen vor der Ausübung einer sicherheitsempfindlichen Tätigkeit voraussetzt. Im Rahmen von Sicherheitsüberprüfungen durch die Geheimschutzbeauftragten wird in diesem Zusammenhang eine Vielzahl personenbezogener Daten zu den Betroffenen zusammengetragen. Sie sind dabei mit einer Sonderstellung ausgestattet, die es ihnen u. a. erlaubt, in Personalakten Einsicht zu nehmen und ihnen ein unmittelbares Vortragsrecht beim Behördenleiter zugesteht. Den von der Sicherheitsüberprüfung Betroffenen stehen aus Gründen des Geheimschutzes im Gegensatz dazu nur eingeschränkte Auskunfts- und Akteneinsichtsrechte zur Verfügung. Um dieses Ungleichgewicht der Tiefe des Eingriffs durch die Sicherheitsüberprüfung einerseits und der Möglichkeiten der Überprüfung von Maßnahmen des Geheimschutzbeauftragten durch den Betroffenen andererseits abzumildern, gibt es das Kontrollrecht des Landesbeauftragten.

Im Berichtszeitraum hat der Landesbeauftragte drei Ministerien einer solchen Kontrolle unterzogen. Darüber hinaus führte er bei einer großen Landesbehörde eine Wiederholungsprüfung durch. Die Ergebnisse der vorhergehenden Kontrolle bedingte bei dieser Stelle eine erneute Überprüfung.

Im Ergebnis der Kontrollen hatte der Landesbeauftragte in allen Fällen Feststellungen zu treffen, die mit datenschutzrechtlichen und/oder sicherheitsüberprüfungsrechtlichen Vorgaben nicht zu vereinbaren waren. In allen Fällen ist der Landesbeauftragte aber auch auf Geheimschutzbeauftragte oder deren Stellvertreter getroffen, die ein Interesse daran haben, die ihnen – ggf. auch nicht immer ganz freiwillig – übertragene Aufgabe verlässlich zu erfüllen. Mit einer solchen Grundeinstellung kann eine Kontrolle durch den Landesbeauftragten sogar oft unerwartet hilfreich sein. Wenn man als Geheimschutzbeauftragter auch im dritten Anlauf beim Haushalt damit scheitert, den erforderlichen Tresor zu beschaffen, hilft es ggf., wenn der Landesbeauftragte die Erforderlichkeit der Anschaffung in seinem Prüfbericht nochmals unterstreicht. Der Landesbeauftragte kann auch darüber hinaus Hinweise geben, wie man praktische Probleme unkompliziert lösen kann. Für eine der geprüften Stellen gestaltete es sich z. B. schwierig, eine technische Lösung für einen abgegrenzten, auch vor Administratorenzugriff geschützten Bereich zur Datenverarbeitung des Geheimschutzbeauftragten zu finden. In Zusammenarbeit mit dem Landesbeauftragten wurde eine praktikable und wirtschaftliche Lösung gefunden. Eine andere Frage, die immer wieder auftaucht, ist die nach der Zugangssicherung zur Sicherheitsakte des Geheimschutzbeauftragten selbst. Wie alle anderen sicherheitsüberprüften Personen darf der Geheimschutzbeauftragte natürlich auch nicht in seine eigene Sicherheitsakte Einsicht nehmen. Er darf sie also nicht selbst bearbeiten. Aber auch hier gibt es einfache Lösungen, die den datenschutzrechtlichen Anforderungen gerecht werden.

Die Erfahrungen zeigen, dass eine Kontrolle auch im Bereich des Geheimschutzes notwendig ist. Da den Betroffenen selbst nur sehr eingeschränkte Rechte zur Verfügung stehen, nimmt der Landesbeauftragte die Kontrolle der Geheimschutzbeauftragten stellvertretend für die Betroffenen wahr. Ziel solcher Kontrollen ist also nicht die sicherheitsüberprüfte Person, sondern die Arbeit des Geheimschutzbeauftragten.

6.8 Novellierung des Melderechts

Bereits im X. (Nr. 6.3), im XI. (Nr. 5.9.1) und im XII. Tätigkeitsbericht (Nr. 6.5.1) hatte der Landesbeauftragte über die bisherigen Novellierungen des Melderechts berichtet und einen Ausblick auf die Neuregelung des Meldewesens gegeben, wonach das bisherige Melderechtsrahmengesetz und das Landesmeldegesetz durch das Bundesmeldegesetz (BMG) abgelöst werden sollen. Der Landesbeauftragte informierte in seinem XII. Tätigkeitsbericht (Nr. 6.5.2 und 6.5.3) über das Ausführungsgesetz des Landes zum Bundesmeldegesetz und über den Aufbau und Betrieb eines zentralen Meldedatenbestandes auf Landesebene (ZMDB).

Im Berichtszeitraum wurde der Landesbeauftragte zu den Entwürfen einer Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden in Sachsen-Anhalt (MeldDÜVO-LSA) und einer Verordnung zum Zentralen Meldedatenbestand des Landes Sachsen-Anhalt (ZMDB-VO LSA) beteiligt.

Der Landesbeauftragte äußerte zum Entwurf der MeldDÜVO-LSA keine grundsätzlichen Bedenken. Die Forderung des Landesbeauftragten, in der ZMDB-VO LSA die Erforderlichkeit im automatisierten Abrufverfahren und deren Zweckbindung unter datenschutzrechtlichen Gesichtspunkten besonders zu berücksichtigen, wurde aufgenommen.

Der ZMDB des Landes Sachsen-Anhalt wird als automatisiertes Verfahren vom Ministerium für Inneres und Sport beim zentralen IT-Dienstleister Dataport in Auftrag gegeben und von Dataport auf einer gemeinsamen IT-Infrastruktur, in der sich auch die Verfahren zu den Zentralen Meldedatenbeständen der Länder Hamburg und Schleswig-Holstein befinden, betrieben. Eine Vor-Ort-Kontrolle in einem zweitägigen Termin am Standort Hamburg durch die Datenschutzbeauftragten der Länder Hamburg, Sachsen-Anhalt und Schleswig-Holstein, unter Anwesenheit eines Vertreters der Bremer Datenschutzbeauftragten, wurde im Frühjahr 2017 durchgeführt (s. Nr. 4.6).

6.9 Personalausweisgesetz

Das Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346) wurde zuletzt durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte bereits im Rahmen der Novellierung darauf hingewiesen, dass das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen werden. In ihrer Entschließung vom Januar 2017 (**Anlage 11**) forderte sie insbesondere, dass Änderungen im Personalausweisgesetz bürger- und datenschutzfreundlich umgesetzt werden.

Im Ergebnis wurden nicht alle Forderungen berücksichtigt. So ist die Aktivierung der eID-Funktion nur dann hinnehmbar, wenn sich daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises ergibt. Künftig entfällt die bisherige Wahlmöglichkeit bei neu ausgestellten Ausweisen, obwohl die Akzeptanz der eID weder bei den Bürgerinnen und Bürgern noch bei Internetanbietern und vielen staatlichen Stellen gegeben ist. Wer künftig ausschließen möchte, dass sein Ausweis zur elektronischen Identifizierung verwendet wird, muss die Aufnahme in eine zentrale Sperrliste veranlassen. Die eID-Funktion auf dem Ausweis bleibt dennoch weiterhin aktiviert.

Neben der Freischaltung der eID-Funktion erlauben die neuen Regelungen im Personalausweisgesetz künftig den Polizeibehörden des Bundes und der Länder, den Verfassungsschutzbehörden des Bundes und der Länder und weiteren Organisationen, das Passfoto „zur Erfüllung ihrer Aufgaben“ im automatisierten Verfahren abzurufen. Nach altem Recht war der Online-Abruf der biometrischen Lichtbilder nur ausnahmsweise zulässig, insbesondere für Zwecke der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten und nur dann, wenn die Personalausweis- bzw. Passbehörde auf andere Weise nicht erreichbar war und ein weiteres Abwarten den Ermittlungszweck gefährdet hätte.

Ob mit der Neuregelung faktisch eine zentrale Datei mit biometrischen Daten eingerichtet wird, bleibt abzuwarten. Zwar gilt das Verbot einer Zentraldatei weiterhin, aber diese Rechtsänderung schafft die Voraussetzungen dafür, dass die verteilten Daten-

bestände der Pass- und Ausweisbehörden online zusammengeschaltet werden. Künftig ist ein Abruf bereits möglich, wenn dieser lediglich zur Erfüllung der Aufgaben z. B. der Sicherheitsbehörden dient.

7 Verfassungsschutz

7.1 Kontrolle der Antiterrordatei

In seinem XII. Tätigkeitsbericht (Nr. 8.3) hat der Landesbeauftragte auf die rechtlichen Rahmenbedingungen zur Kontrolle der Antiterrordatei hingewiesen. Er ist nach § 10 Abs. 2 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (ATDG) dazu verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes zu kontrollieren.

Diese Verpflichtung trifft den Landesbeauftragten sowohl für die Verfassungsschutzbehörde des Landes Sachsen-Anhalt als auch für das Landeskriminalamt Sachsen-Anhalt. Beide Stellen sind aufgrund von § 1 Abs. 1 ATDG an der Antiterrordatei beteiligt. Sie tragen jeder für die jeweils in der Antiterrordatei gespeicherten Daten die datenschutzrechtliche Verantwortung und sind deshalb Adressat der Kontrollen des Landesbeauftragten.

Der Landesbeauftragte ist seiner Verpflichtung nachgekommen und hat im Jahre 2017 die Durchführung des Datenschutzes bei der Antiterrordatei sowohl bei der Verfassungsschutzbehörde des Landes als auch beim Landeskriminalamt kontrolliert. Im Ergebnis konnte er feststellen, dass in Bezug auf die konkreten Kontrollgegenstände keine datenschutzrechtlich zu beanstandenden Speicherungen durch die verantwortlichen Stellen vorgenommen wurden.

7.2 Beobachtung der Reichsbürgerszene

Wie aus der Presseberichterstattung, aber auch aus dem Verfassungsschutzbericht des Landes Sachsen-Anhalt für das Jahr 2016 zu entnehmen war, wird die sog. Reichsbürgerszene durch die Verfassungsschutzbehörde des Landes Sachsen-Anhalt beobachtet. Nach dem Verfassungsschutzbericht soll durch die Beobachtung sowohl eine quantitative als auch qualitative Bewertung der Reichsbürgerszene vorgenommen werden.

Aufgrund eines Übermittlungsersuchens der Verfassungsschutzbehörde des Landes Sachsen-Anhalt an die obersten Landesbehörden und durch Erlasse des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt (MI) wurden Grundlagen für Datenübermittlungen an die Verfassungsschutzbehörde geschaffen und ausdrücklich auf die bestehende Rechtslage hingewiesen.

Der Landesbeauftragte hat zu der Frage der Übermittlung und Speicherung personenbezogener Daten in Bezug auf „Reichsbürger“ sowohl die für die Polizei zuständige Abteilung des MI als auch die Verfassungsschutzbehörde des Landes Sachsen-Anhalt ausgiebig beraten. Bei letzterer wurde auch vor Ort geprüft, inwieweit Speicherungen zu „Reichsbürgern“ dem Grunde nach zulässig erfolgen. Die dazu vorge-

legten Stellungnahmen und die Einsichtnahme in gespeicherte personenbezogene Daten zu „Reichsbürgern“ gaben keinen Anlass zu Beanstandungen.

8 Rechtspflege und Justizvollzug

8.1 Vorratsdatenspeicherung

Bereits in seinem XII. Tätigkeitsbericht (Nr. 7.1) hatte der Landesbeauftragte über den Gesetzentwurf und die Verabschiedung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten berichtet. Das Gesetz, welches am 18. Dezember 2015 in Kraft getreten ist (BGBl. I S. 2218), verpflichtet Erbringer öffentlich zugänglicher Telefon- und Internetzugangsdienste, spätestens ab dem 1. Juli 2017 Verkehrsdaten ihrer Nutzer gem. § 113b Abs. 2 und 3 Telekommunikationsgesetz (TKG) für 10 Wochen und Standortdaten gem. § 113b Abs. 4 TKG für 4 Wochen anlasslos zu speichern und diese bei Bedarf an die in § 113c Abs. 1 Nrn. 1 und 2 genannten Behörden zu übermitteln oder für eine Auskunft nach § 113 Abs. 1 Satz 3 TKG bereitzustellen.

Allerdings hat der Europäische Gerichtshof mit Urteil vom 21. Dezember 2016 in zwei verbundenen Vorabentscheidungsverfahren (Az.: C-203/15; C-698/15; NJW 2017, 717) klargestellt, dass eine nationale Regelung, die eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien zulässt, nicht mit Unionsrecht vereinbar sei. Konkret heißt das, dass sich die nationalen Regelungen auf das absolut Notwendige zu beschränken haben und diese Beschränkung nicht erst für den behördlichen Zugriff darauf, sondern schon für die Speicherung der Daten gilt.

Die Gesamtheit der Daten, die im Rahmen der Vorratsdatenspeicherung erfasst werden, erlaube sehr genaue Rückschlüsse auf das Privatleben der Nutzer, weshalb der damit verbundene Grundrechtseingriff als besonders schwerwiegend anzusehen sei. Gerade der Umstand, dass die Daten ohne Information der Nutzer erhoben würden, könne bei diesen ein Gefühl der ständigen Überwachung erzeugen. Ausnahmen könne es daher nur bei der Bekämpfung von schweren Straftaten geben, wobei die überwachten Personen im Verdacht stehen müssen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder in eine solche verwickelt zu sein.

Bereits 2014 hatte der Europäische Gerichtshof die EU-Richtlinie 2006/24/EG über die Vorratsdatenspeicherung für ungültig erklärt. Grund war damals ebenfalls, dass die darin vorgeschriebene Verpflichtung von Telekommunikationsanbietern, die Daten ihrer Nutzer zu speichern, nicht auf das Notwendige beschränkt gewesen war.

In einem Beschluss vom 22. Juni 2017 entschied das Oberverwaltungsgericht Nordrhein-Westfalen (Az. 13 B 238/17) im einstweiligen Verfahren, dass das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten nicht mit Unionsrecht vereinbar ist. Das Gericht führte hierzu aus, dass die Speicherpflicht infolge des Urteils des Europäischen Gerichtshofs vom 21. Dezember 2016 – jedenfalls in ihrer gegenwärtigen Ausgestaltung – nicht mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG (E-Privacy-Richtlinie) vereinbar sei, da sie pauschal die Verkehrs- und Standortdaten aller Nutzer von Telefon- und Internetdiensten erfasse. Eine Beschränkung des betroffenen Personenkreises fehle. Es stellte weiterhin fest, dass der klagende Internet-Diensteanbieter bis zum rechtskräftigen Abschluss des Haupt-

sacheverfahrens nicht verpflichtet ist, die in § 113b Abs. 3 TKG genannten Verkehrsdaten zu speichern. Das VG Köln schloss sich mit Urteil vom 20. April 2018 (Az. 9 K 3859/16) dieser Rechtsauffassung an.

Die Bundesnetzagentur sieht einstweilen von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab und leitet auch keine Bußgeldverfahren ein.

Die Vorratsdatenspeicherung bleibt weiterhin maßgeblicher Testfall für das Verhältnis von Freiheit und Sicherheit. Durch anlasslose Massenspeicherungen alle Telefon- und Internetnutzer unter Generalverdacht zu stellen, erhöht nicht die Sicherheit und ist grundrechts- und demokratiewidrig.

8.2 Elektronischer Rechtsverkehr in der Justiz

Der Landesbeauftragte hatte in seinem XII. Tätigkeitsbericht (Nr. 7.4) über die Aktivitäten der Justizverwaltung des Landes zur Einführung des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akte (eAkte) sowie über den Aufbau einer entsprechenden 3-stufigen Projektorganisation unter Federführung des Ministeriums für Justiz und Gleichstellung (MJ) berichtet.

Der Landesbeauftragte begleitet diesen Prozess der Einführung des ERV und der eAkte, u. a. als Mitglied dieser Gremien. Dem Strategiegremium unter Leitung des Staatssekretärs des MJ angeschlossen war der Lenkungskreis, der wiederum die Aufgabenumsetzung in den gebildeten sechs Arbeitsgruppen koordinierte. Im Juni 2017 erfolgte durch das zuständige MJ eine Umstrukturierung der ERV-Projektorganisation durch eine Aufteilung in eine strategische und eine operative Ebene. Hierzu wurde das Strategiegremium in einen Projektlenkungsausschuss (PLA) mit dem Staatssekretär des MJ als Auftraggeber und gleichzeitigem Mitglied umgewandelt. Der PLA fungiert als oberste Entscheidungs- und Kontrollinstanz. Der Landesbeauftragte ist Mitglied in diesem PLA, jedoch nicht stimmberechtigt. Die Projektleitung übernimmt die operative Führung des Projekts. Im Zuge der Reorganisation der Arbeitsgruppen wurde ein Projekt-Kernteam eingerichtet, welches konkrete Einzelthemen in Form von Teilprojekten bearbeitet, die Arbeitsgruppen Staatsanwaltschaften und Justizvollzug integriert sowie die laufenden Pilot- und Rolloutprojekte einbezieht.

Die Einführung des ERV in Sachsen-Anhalt und seine Umsetzung konzentriert sich dabei auf drei Schwerpunktbereiche bzw. gemeinsame Entwicklungsverbünde der Länder an denen auch das Land Sachsen-Anhalt beteiligt ist:

e^2-Verbund, in welchem sich die Länder Bremen, Niedersachsen, Nordrhein-Westfalen, Hessen, Saarland und Sachsen-Anhalt zu einem gemeinsamen Entwicklungs- und Pflegeverbund im Hinblick auf den elektronischen Rechtsverkehr und die elektronische Aktenführung zusammengeschlossen haben. „e^2“ steht dabei für den Anspruch, „ergonomisch-elektronisch“ zu sein, d. h. ergonomisch wie elektronisch optimale Arbeitsumgebungen zu schaffen. Die Erarbeitung der „e^2-Module“ erfolgt arbeitsteilig zwischen den Ländern:

- e^2A – eAkte, Aktenbearbeitungsumgebung (Nordrhein-Westfalen),
- e^2T – Textverarbeitungssystem (Niedersachsen),
- e^2P – Posteingangs-/Postausgangs-Management (Hessen) sowie
- e^2S – Saalanzeige- und Managementsystem (Sachsen-Anhalt).

Die Programme des e^2-Verbunds sollen zu Beginn in Kombination mit den in den Ländern vorhandenen Fachanwendungen genutzt werden. Für die Zukunft ist bundesweit die Entwicklung eines „einheitlichen Fachverfahrens“ geplant. Es soll nicht nur in der ordentlichen Gerichtsbarkeit, sondern auch in den Staatsanwaltschaften und den Fachgerichtsbarkeiten die unterschiedlichen Verfahren ersetzen, die heute in Bund und Ländern genutzt werden. Später soll das künftige „einheitliche Fachverfahren“ die Altverfahren ablösen.

EUREKA-Fach, das Programmpaket, welches der Automationsunterstützung in den Verfahren der Verwaltungs-, Arbeits-, Sozial- und Finanzgerichtbarkeit dient und flexibel an künftige Entwicklungen und Erfordernisse des ERV angepasst werden soll. Vierzehn Bundesländer, darunter auch Sachsen-Anhalt, haben sich bisher für den Einsatz von EUREKA-Fach entschieden. Im Jahr 2017 wurde ein Verbundmanagement des EUREKA-Fach Länderverbundes (mit Sitz beim OVG Lüneburg) eingerichtet.

web.sta, als Fachverfahren im Geschäftsbereich der Staatsanwaltschaften bietet es ein vollständiges webbasiertes Informationssystem, welches über den Stand von Ermittlungsverfahren, die gerichtliche Terminierung und über den Stand der Vollstreckung Auskunft gibt. Die Entwicklung erfolgte in einem aus neun Bundesländern bestehenden Verbund, in dem Bayern die Federführung obliegt. Weiterhin gehören dem Verbund Baden-Württemberg, Bremen, Niedersachsen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Thüringen an.

Gemäß dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) war der elektronische Zugang ab dem 1. Januar 2018 zu allen deutschen Gerichten zu ermöglichen. Mit der Herstellung der elektronischen Empfangsbereitschaft aller Gerichte und Staatsanwaltschaften wurde der ERV flächendeckend eröffnet und in einer 1. Ausbaustufe, die zumindest diese gesetzlichen Mindestanforderungen der Einführung des ERV in der Justiz Sachsen-Anhalts umsetzt, realisiert. In der 2. Ausbaustufe wird es um die elektronische Versandbereitschaft gehen.

Zur Vermeidung von Medienbrüchen ist die Einführung des elektronischen Rechtsverkehrs untrennbar mit der Einführung der elektronischen Akte verbunden. Diese soll zukünftig eine durchgehende elektronische Aktenbearbeitung vom Eingang eines Dokuments bis zur Versendung einer Entscheidung ermöglichen und damit erst wirklich die Vorteile des elektronischen Rechtsverkehrs optimal nutzen.

Der Bundesgesetzgeber hat mit dem Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 (BGBl. I S. 2208) und der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV) vom 24. November 2017 (BGBl. I S. 3803, zuletzt geändert durch Artikel 1 der Verord-

nung vom 9. Februar 2018 (BGBl. I S. 200)) dafür die gesetzlichen Voraussetzungen geschaffen.

Im Bereich der Justiz Sachsen-Anhalts erfolgt die Pilotierung der eAkte im Finanzgericht des Landes in Dessau-Roßlau.

Die Nutzung des „Elektronischen Gerichts- und Verwaltungspostfaches“ (EGVP) für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften des Landes Sachsen-Anhalt wird ergänzt durch das besondere elektronische Anwaltspostfach (beA) für die Anwaltschaft. Hierbei gab es technische Umsetzungsprobleme. Für die Anwaltschaft soll das beA frühestens ab September 2018 zur Verfügung stehen. Die prognostizierten hohen Eingangszahlen elektronischer Dokumente ab dem 1. Januar 2018 blieben auch aufgrund der Verschiebung der Inbetriebnahme des beA weit hinter den Erwartungen zurück.

Mit der Einführung des besonderen elektronischen Behördenpostfachs (beBPo) soll für die Behörden des Landes ebenfalls die Grundlage für einen sicheren Kommunikationsweg geschaffen werden. Als beBPo-Prüfstelle wurde durch Kabinettsbeschluss Dataport bestimmt. Die Regelungen für das Zertifizierungsverfahren für das beBPo werden vom MJ mit dem MI und dem MF abgestimmt. Der vom MJ angekündigte Erlass zum beBPo hierzu stand bei Redaktionsschluss noch aus.

Auch bei einer zukünftigen elektronischen Aktenführung sind die Anforderungen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) und der JI-Richtlinie (Richtlinie (EU) 2016/680 vom 27. April 2016) zu berücksichtigen. Die Ausarbeitung eines Justiz-IT-Gesetzes des Landes, wie im Koalitionsvertrag der 7. Legislaturperiode vereinbart, steht noch aus. In diesem Gesetz sollen die Organisation und Betreuung der Informations- und Kommunikationstechnik der Gerichte und der Staatsanwaltschaften einschließlich bereichsspezifischer Datensicherheits- und Datenschutzanforderungen geregelt werden.

Zweifel sind angebracht, inwieweit die im April 2017 seitens des MJ vorgenommene Veränderung der Projektorganisation den Gesamtprozess der Einführung des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akte (eAkte) beschleunigen kann. Die bestehenden personellen Defizite bei der ADV-Stelle der Justiz und auch in den einzelnen Projekten und selbst im Bereich des Projektmanagements selbst lassen sich nicht mit neuen Strukturen beheben. Bedenken bestehen auch bezüglich der Zukunft des Justiz-Rechenzentrums in Barby, inwieweit es technisch und personell für diese komplexen Aufgaben des ERV aufgestellt ist. Die Verzögerung der Inbetriebnahme des ITN-XT (siehe Nr. 4.2) stellt sich als ein weiteres grundlegendes Problem für die Einführung des ERV in Sachsen-Anhalt dar.

8.3 PPP-Projekt Justizvollzuganstalt Burg

Seit 2007 besteht im Zusammenhang mit der Ausarbeitung eines Datenschutzkonzepts für die Justizvollzugsanstalt Burg mit dem Ministerium für Justiz und Gleichstellung (MJ) eigentlich Einvernehmen darüber, dass es sich bei der Erhebung, Verarbeitung und Nutzung durch den privaten Dienstleister um Auftragsdatenverarbeitung handelt (vgl. Nr. 7.3 des XI. Tätigkeitsberichts). Das Konzept der Teilprivatisierung

beruht dabei darauf, dass der private Bereich einem verbeamteten Controller untersteht, der gegenüber dem privaten Partner weisungsbefugt ist. Der private Partner wird im Auftrag der JVA Burg als Verwaltungshelfer tätig. Dies hatte das MJ immer wieder betont.

Bereits im Jahr 2006 hatten die Länder mit der Föderalismusreform die Gesetzgebungskompetenz für den Strafvollzug erhalten, jedoch galt das Strafvollzugsgesetz des Bundes bis zum Inkrafttreten von Ländergesetzen fort. In letzterem fehlte allerdings eine Rechtsgrundlage für die Auftragsdatenverarbeitung. Der teilprivatisierte Betrieb der JVA Burg war also wegen dieser Regelungslücke datenschutzrechtlich problematisch. Deshalb hatte der Landesbeauftragte angemahnt, so schnell wie möglich eine entsprechende Rechtsgrundlage in einem Strafvollzugsgesetz des Landes zu schaffen. Im Vorgriff auf die notwendigen Regelungen hatte er den Abschluss eines Vertrags über die Auftragsdatenverarbeitung empfohlen.

Der Landesgesetzgeber ist seinen Empfehlungen letztendlich gefolgt und hat in das Justizvollzugsgesetzbuch Sachsen-Anhalt (JVollzGB LSA) speziell mit Blick auf das PPP-Projekt JVA Burg Regelungen für die Auftragsdatenverarbeitung aufgenommen. Der Einsatz des privaten Partners setzt voraus, dass die Parteien einen Vertrag über die Auftragsdatenverarbeitung schließen bzw. geschlossen haben, der den Anforderungen der §§ 109, 163 JVollzGB LSA i. V. m. § 8 DSG LSA genügt. Der private Partner ist weisungsgebunden und wird grundsätzlich als Verwaltungshelfer tätig. Die Ausübung hoheitlicher Tätigkeiten ist ihm ausdrücklich untersagt, § 109 Abs. 1 Satz 4 JVollzGB LSA.

Im Vertragswerk zum PPP-Projekt JVA Burg fehlte allerdings von Anfang an ein Vertrag über die Auftragsdatenverarbeitung. Da der private Partner nicht nur in einem, sondern in verschiedenen Bereichen tätig wurde, hatte der Landesbeauftragte den Parteien den Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung nahegelegt. Ziel der Beratungs- und Kontrolltätigkeit des Landesbeauftragten war es also, die Verarbeitung personenbezogener Daten des privaten Dienstleisters im Auftrag der JVA Burg rechtlich abzusichern.

Diese Bemühungen schienen zunächst Früchte zu tragen, denn die Landesregierung hatte in ihrer Stellungnahme zum XI. Tätigkeitsbericht vom 1. Oktober 2014 mitgeteilt, dass die erforderlichen vertraglichen Regelungen mit dem privaten Partner abgestimmt würden (LT-Drs. 6/3512). Der Abschluss des erforderlichen Generalvertrags über die Auftragsdatenverarbeitung schien also mit einiger Verspätung auf den Weg gebracht worden zu sein. Dafür sprach auch, dass die Datenschutzdienstanweisungen in der JVA Burg unter Berücksichtigung der Rechtsauffassung des Landesbeauftragten bereits überarbeitet worden waren.

Nachdem zwei Jahre später immer noch kein neues Vertragswerk vorlag, hatte der Landesbeauftragte in seinem XII. Tätigkeitsbericht (Nr. 7.3) erneut auf die Notwendigkeit des Abschlusses eines Generalvertrags über die Auftragsdatenverarbeitung hingewiesen und kritisiert, dass das MJ die Herbeiführung eines rechtskonformen Zustands nicht nachhaltig verfolge. Dem widersprach die Landesregierung in ihrer Stellungnahme vom Februar 2017 nicht.

Völlig überraschend hat das MJ dem Landesbeauftragten im Mai 2017 mitgeteilt, dass es die Tätigkeit des privaten Partners in der JVA Burg datenschutzrechtlich neu

bewerten wolle. Anknüpfungspunkt für die neue Bewertung sei das JVollzGB LSA. Obwohl mit diesem ausdrücklich die Rechtsgrundlage für die Auftragsdatenverarbeitung geschaffen worden war, um die Tätigkeit des privaten Dienstleisters in der JVA Burg gesetzlich zu regeln, wollte das MJ auf diese nicht zurückgreifen. Es hat vielmehr vorgetragen, dass mit dem neuen Gesetz auch Regelungen für die Datenübermittlung aufgenommen worden seien. Der private Partner plane und führe seine Arbeitsschritte eigenverantwortlich aus. Und geradezu verblüffend: Die Aufgabenerfüllung erfolge auch nicht nach Weisung. In enger Abstimmung mit dem privaten Partner sei man daher zu dem Ergebnis gekommen, dass es sich nicht um eine Verarbeitung personenbezogener Daten im Auftrag, sondern um eine Datenübermittlung handele. Der Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung sei daher nicht mehr notwendig.

Der Landesbeauftragte hat dieser Auffassung ausdrücklich widersprochen. Es liegt keine neue Sach- und Rechtslage vor, denn schon dem alten Recht lag die Unterscheidung zwischen Auftragsdatenverarbeitung und Datenübermittlung zugrunde. Durch das Inkrafttreten des JVollzGB LSA hat sich schließlich auch nicht das Konzept der Teilprivatisierung geändert. Vielmehr hat die Landesregierung in der Begründung des Gesetzentwurfs zur Weiterentwicklung des Justizvollzugs in Sachsen-Anhalt noch einmal klargestellt, dass der private Dienstleister im Rahmen einer Beauftragung agiere. Wenn er im Rahmen des Auftrags bei der Absuchung von Besuchern tätig werde, stehe er unter ständiger Aufsicht eines staatlichen Bediensteten, sodass die Anstalt jederzeit Einfluss auf sein Handeln nehmen könne. Der private Partner werde daher lediglich als Werkzeug (Verwaltungshelfer) tätig (LT-Drs. 6/3799). Schließlich waren aufgrund der datenschutzrechtlichen Bedenken des Landesbeauftragten die dem privaten Partner im Rahmen der Besucherkontrolle übertragenen Aufgaben noch enger gefasst worden, um deutlich zu machen, dass der private Partner in diesem Bereich ausschließlich weisungsgebundene Hilfstätigkeiten unter ständiger Aufsicht staatlicher Bediensteter wahrnehme (LT-Drs. 6/3512 zu Nr. 7.3 und Nr. 7.4).

Etwas Anderes würde sich nur ergeben, wenn das MJ bzw. die JVA Burg in Absprache mit dem privaten Partner dessen Aufgabenbereich ohne Abstimmung mit dem Parlament und entgegen der dem Landesbeauftragten gegebenen Zusagen eigenmächtig erweitert hätte. Der Landesbeauftragte geht davon aus, dass dies nicht erfolgt ist, sodass der Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung nach wie vor erforderlich ist.

Der Landesbeauftragte erwartet, dass das Ministerium für Justiz und Gleichstellung seine Rechtsauffassung überprüft und den Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung endlich auf den Weg bringt.

9 Forschung, Hochschulen und Schulen

9.1 Forschung und Hochschulen

Der Forschungsbereich war wiederum ein arbeitsintensiver Schwerpunkt. Der Landesbeauftragte wurde im Berichtszeitraum bei 21 neuen und einigen Langzeitforschungsprojekten beteiligt. Die komplexen Studien waren zumeist im medizinischen Bereich, aber auch in den Bereichen Wirtschaft, Soziales und Polizei angesiedelt. Im

Bildungsbereich wurden dem Landesbeauftragten sowohl einige neue als auch durch anstehende Erhebungswellen wiederkehrende Forschungsprojekte zur datenschutzrechtlichen Bewertung vorgelegt. Insbesondere bei der Begleitung des Forschungsprojektes des Nationale Kohorte e. V. (NAKO e.V.) kamen in diesem Berichtszeitraum mehrere Besuche vor Ort hinzu.

9.1.1 Nationale Kohorte

Wie im XII. Tätigkeitsbericht (Nr. 9.1.3) angekündigt, hat der Landesbeauftragte in diesem Berichtszeitraum in beiden in Sachsen-Anhalt an dieser großen, bundesweiten, medizinischen Langzeitstudie (geplant 200.000 Probanden) beteiligten Einrichtungen (das Studienzentrum in Halle und das Kompetenzzentrum Sekundärdaten in Magdeburg) vor Ort Informations- und Beratungsbesuche durchgeführt.

Im Studienzentrum (Erhebung von Probandendaten), das bereits im Mai 2014 mit den Untersuchungen begonnen hatte, wurden insbesondere die Verfahrensabläufe, die verwendeten Einladungsschreiben und Fragebögen und das lokale Datenschutzkonzept diskutiert. Der Landesbeauftragte hat u. a. empfohlen, die Angaben zu den Gründen einer Nichtteilnahme mittels Fragebogen anonym zu erheben. Auch wurde angemahnt, alsbald die vorgesehene zentrale Speicherung der diagnostischen Daten im „Integrationszentrum“ in Greifswald zu ermöglichen und danach im Studienzentrum nicht mehr erforderliche Informationen zu löschen. Die Hinweise wurden an die Geschäftsstelle des NAKO e. V. weitergeleitet.

Im Kompetenzzentrum Sekundärdaten (Abgleich mit anderen Datenbeständen), dem bisher noch keine Daten zu Verfügung stehen, wurden das Datenschutz- und IT-Sicherheitskonzept des Kompetenznetzwerkes Sekundär- und Registerdaten der NAKO e. V. und das Datenschutzkonzept des Institutes für Sozialmedizin und Gesundheitsökonomie erörtert. Wenn Daten von den Krankenversicherungen abgefordert werden, erfolgt dies ausschließlich in pseudonymer Form. Eine Datenspeicherung erfolgt lediglich temporär.

9.1.2 Bescheinigung der Prüfungsunfähigkeit

Häufig wird von Studierenden die Frage gestellt, in welchem Umfang Prüfungsausschüsse der Hochschulen medizinische Informationen zur Beurteilung der Prüfungsunfähigkeit anfordern dürfen. Ein Austausch mit einzelnen Datenschutzbeauftragten der Hochschulen und einzelnen Prüfungsausschüssen hat in den letzten Jahren stattgefunden. Hierzu hat der Landesbeauftragte folgende Hinweise gegeben:

Die Prüfungsunfähigkeit ist eine vom Prüfungsausschuss zu entscheidende Rechtsfrage. Er entscheidet abschließend und eigenverantwortlich über die Anerkennung des Entschuldigungsgrundes. Es ist jedoch zu berücksichtigen, dass in den meisten Prüfungsausschüssen keine medizinische Fachkompetenz vertreten sein dürfte. Die Feststellung einer medizinisch begründeten prüfungsbezogenen Leistungsunfähigkeit ist nur Aufgabe des Arztes. Auch sind die verfassungsrechtlichen Vorgaben der Erforderlichkeit sowie der Datensparsamkeit zum Schutze des Persönlichkeitsrechts der Prüfungskandidaten zu berücksichtigen.

Es sollten Vordrucke für ärztliche Atteste mit entsprechenden Erläuterungen verwendet werden. Darin sollte die Form der abzulegenden Prüfung beschrieben werden, um die Relevanz der Leistungsunfähigkeit erkennen zu können (z. B. Armbruch bei schriftlicher oder mündlicher Prüfung). Auf die Notwendigkeit der Beschreibung der krankheitsbedingten Einschränkungen könnte hingewiesen werden. Ebenso können weitere wesentliche Aspekte erfragt werden, z. B. akute und unaufschiebbare Erkrankung, vorübergehender Charakter, Ausschluss von Examenspsychosen. Weiterhin sollte ausdrücklich darauf hingewiesen werden, dass die Angaben von Diagnosen und detaillierten medizinischen Informationen z. B. in Form von Gutachten grundsätzlich nicht erforderlich sind.

Soweit der Arzt die Befugnis erhalten soll, die Informationen direkt an den Prüfungsausschuss zu übermitteln, bedarf er einer Offenbarungsbefugnis (siehe § 203 StGB, Schweigepflichtentbindung).

Prüfungsausschüsse benötigen hinreichende Informationen, um eine krankheitsbedingte Leistungsbeeinträchtigung nachvollziehen zu können. Diagnosen gehören grundsätzlich nicht dazu.

9.2 Schulwesen

9.2.1 Behördliche Datenschutzbeauftragte in Schulen

Bereits seit dem Jahr 2011 setzt sich der Landesbeauftragte intensiv dafür ein, dass die gesetzliche Bestellungsverpflichtung für behördliche Datenschutzbeauftragte in Schulen umgesetzt wird. Seit dem Jahr 2012 ist das für Bildung zuständige Ministerium des Landes Sachsen-Anhalt über den erheblichen Handlungsbedarf informiert (vgl. Nr. 9.3.1 des XI. Tätigkeitsberichtes und Nr. 9.2.1 des XII. Tätigkeitsberichtes). Eine konkretisierende bzw. unterstützende Regelung für die Schulen ist jedoch noch immer nicht in Kraft getreten.

Im Februar 2016 ist der Landesbeauftrage vom damaligen Kultusministerium des Landes Sachsen-Anhalt darüber informiert worden, dass nunmehr für die Schulen in freier Trägerschaft eine Verordnung die Arbeit der schulischen Datenschutzbeauftragten regeln soll. Für die staatlichen Schulen wurde nur ein Erlassentwurf vorgelegt, der im Wesentlichen dem Stand der Beratungen vom Oktober 2014 entsprach. Eine Veröffentlichung dieses Erlasses wurde für April 2016 in Aussicht gestellt. Während einer Beratung mit dem Ministerium für Bildung des Landes Sachsen-Anhalt (MB) im Mai 2016 wurde dann allerdings mitgeteilt, dass das Ministerium doch für alle Schulen in Erlassform agieren wolle. Die für Juli 2016 in Aussicht gestellte Veröffentlichung fiel dann wegen fachlicher Einwendungen und weiteren Überarbeitungen aus.

Im Juli 2017 wandte sich das MB mit Fragen im Zusammenhang mit der DS-GVO an den Landesbeauftragten. Der Landesbeauftragte teilte dem MB daraufhin mit, dass gegen den im Juni 2016 übersandten und abgestimmten Erlassentwurf aus seiner Sicht auch in Bezug auf die DS-GVO keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen. Er wies erneut auf die in den Schulen festgestellten Datenschutzverstöße hinsichtlich der verpflichtenden Bestellung behördlicher Datenschutzbeauftragter hin.

Das MB plant nunmehr die Schaffung von vier neuen Stellen im Landesschulamt Sachsen-Anhalt. Sofern diese im Haushaltsplan für 2019 berücksichtigt werden, sollen die Aufgaben des Datenschutzbeauftragten von dort für die Schulen in Sachsen-Anhalt erfüllt werden.

Obwohl das Ministerium für Bildung des Landes Sachsen-Anhalt bereits seit dem Jahr 2012 darüber informiert ist, dass in den Schulen Sachsen-Anhalts hinsichtlich der gesetzlichen Bestellungspflicht für behördliche Datenschutzbeauftragte erheblicher Handlungsbedarf besteht, ist es diesem in den vergangenen sechs Jahren nicht gelungen, die Vorgaben für die Schulen umzusetzen. Die Fortdauer dieses Zustandes ist mit einem sachgerechten Umgang mit den Persönlichkeitsrechten von Schülerinnen und Schülern nicht zu vereinbaren.

9.2.2 Schulgesetz und Schuldatenverordnung

Mit einem Vorlauf von wenigen Tagen war der Landesbeauftragte um Stellungnahme zu einem Schulgesetzentwurf angehört worden, der in datenschutzrechtlicher Hinsicht eine Anpassung an die Vorgaben der Europäischen Datenschutz-Grundverordnung (DS-GVO) enthielt. Da eine so kurzfristige Stellungnahme nicht möglich war, hat sich der Landesbeauftragte im Rahmen einer Anhörung durch den Bildungsausschuss des Landtages im Dezember 2017 positioniert (LT-Drs. 7/1992). Zu einzelnen vorgesehenen Anpassungsregelungen im Hinblick auf die DS-GVO wurde auf das grundsätzliche europäische Normwiederholungsverbot hingewiesen. Bezüglich einer Regelung zur Befugnis von Gesundheitsbehörden wurde angeregt, wegen der engen Vorgaben von Art. 9 DS-GVO ausdrücklich die Verarbeitung von besonderen Kategorien von Daten aufzunehmen. Weitere Empfehlungen bezogen sich u. a. auf das Verarbeiten von Daten durch Lehrkräfte außerhalb der Schule.

Besonders problematisch erschien eine Vorschrift zur verpflichtenden Anbindung von Schulen an ein landesweit einheitliches IT-gestütztes Schulverwaltungsverfahren bzw. Bildungsmanagementsystem zur Vereinfachung von übergreifenden Schulverwaltungsaufgaben (vgl. dazu unter Nr. 9.2.3). Hierzu bestanden schon verfassungsrechtliche Bedenken, da gesetzlich ein IT-System vorgegeben würde, das in der gewünschten Form noch nicht entwickelt war. Deshalb war die gebotene Technik-Folgenabschätzung des Landtages im Hinblick auf die Grundrechte der von der Anwendung Betroffenen nicht möglich. In Bezug auf die geplante einheitliche Infrastruktur wurde dazu seitens des Landesbeauftragten auf die Notwendigkeit hingewiesen, die Schulverwaltungssoftware kennen zu müssen, um ein geplantes Bildungsmanagementsystem mit Aspekten der Steuerung, des Monitorings und der Statistik beurteilen zu können. Auch war der Umfang der im Bildungsmanagementsystem geplanten Datensammlung bedenklich, da nicht nur Schulverwaltungsdaten, sondern auch Organisations-, Statistik- und Planungsdaten einbezogen werden sollen.

In den sich anschließenden Beratungen mit dem Bildungsministerium wurden daher weitere Empfehlungen gegeben. Einmal sollte das zentrale IT-Verfahren näher erläutert werden. Auch sollte im Gesetzestext die Vorgabe des Bildungsministeriums verdeutlicht werden, dass nicht mehr Daten verarbeitet werden dürfen, als bisher. Die Maßgaben der Datenverarbeitung aus den bestehenden Regelungen sollten nicht erweitert werden. Eine die Empfehlungen des Landesbeauftragten einbeziehende Fassung (s. § 84f SchulG LSA) ist zwischenzeitlich im Landtag beschlossen worden

(Vierzehntes Gesetz zur Änderung des Schulgesetzes vom 24. Juli 2018, GVBl. LSA S. 224).

Die §§ 84a bis 84e SchulG LSA enthalten Verordnungsermächtigungen. Das Bildungsministerium hat dem Landesbeauftragten im Sommer 2015 den Entwurf einer Schuldatenverordnung übersandt. Sie enthält u. a. Ausführungen zur Zulässigkeit der Datenverarbeitung, zur Verarbeitung auf privaten Geräten, zu Statistiken, Maßnahmen zur Datensicherheit und zum Datenbestand in Schulen und Schulbehörden. In Anlagen zum Verordnungstext sollte der Datenbestand detailliert aufgeführt und konkreten Zweckbestimmungen zugeordnet werden. Der Landesbeauftragte wies in mehreren Beratungen umfänglich auf datenschutzrelevante Aspekte, Unstimmigkeiten und Optimierungsmöglichkeiten hin.

Dieser Entwurf enthält auch Regelungen zum Umgang mit Personaldaten der Lehrkräfte. Hierzu wurde auf die Konkurrenz zu den Regelungen im Beamtenrecht, ggf. i. V. m. § 28 Abs. 1 DSG LSA, hingewiesen. Auch begegnete die fünf Jahre lange Speicherung von Unterlagen zu disziplinarischen Angelegenheiten Bedenken im Hinblick auf die Vorgaben von § 89 Abs. 1 LBG LSA und § 16 Abs. 5 DG LSA. Zur Nutzung privater digitaler Geräte durch Lehrkräfte wurde erläutert, dass § 84a Abs. 7 SchulG LSA als Ausnahmeregelung nur einen engen Rahmen biete, sodass die vorgesehene Formulierung zu einer weitreichenden Nutzung wohl einer Grundlage entbehre. Bemängelt wurde auch, dass die für die Speicherung in der automatisierten zentralen Schülerdatei nach § 84c Abs. 1 Nr. 10 SchulG LSA vorgesehenen „Schulpflichtmerkmale“ keine Konkretisierung erfuhren. Klärungsbedarf ergab sich auch hinsichtlich zu der in den Anlagen aufgeführten Schülernummer. Viele Fragestellungen ergaben sich weiter zu den Regelungen im Statistikbereich, insbesondere in Bezug auf die Gewährleistung des Statistikgeheimnisses und das Löschungsverfahren.

Nach umfangreichen Beratungen im Sommer 2016 teilte das Bildungsministerium Anfang 2017 mit, dass noch inhaltliche und technische Abstimmungen in der Schulverwaltung notwendig seien. Das Vorhaben wurde zumal infolge der oben dargestellten Schulgesetznovelle zurückgestellt. Damit ist die Schuldatenverordnung zu den §§ 84a bis 84e SchulG LSA seit Ende 2012 überfällig.

Die Umsetzung der gesetzlichen Vorgaben zum Schutz des Persönlichkeitsrechts von Schülerinnen und Schülern sowie Lehrkräften wirft in der konkreten Praxis des Schulalltags häufig Anwendungsfragen auf. Zur Unterstützung der Praxis hat das Bildungsministerium mit Beratung des Landesbeauftragten zum Schuljahresbeginn 2018/2019 eine umfängliche Handreichung „Datenschutz an Schulen“ erarbeitet.

9.2.3 Bildungsmanagementsystem

Bei dem Bildungsmanagementsystem handelt es sich um ein zentrales, landeseinheitliches Softwareprodukt, das der prozessoptimierten Steuerung des Schulbetriebes dienen soll. Das Anwendungsspektrum reicht vom lokalen Schulbetrieb über die politische Steuerung von Verwaltungs- und Planungsprozessen bis zu statistischen Erhebungen. Das Bildungsmanagementsystem bezieht sich nicht auf die pädagogische Komponente digitaler Bildung. Der Landesbeauftragte wird vom Bildungsministerium bei der Planung und Umsetzung einbezogen.

In Beratungen konnte er auf notwendige Optimierungen im Hinblick auf die gesetzlichen Grundlagen (s. Nr. 9.2.2) und auf materielle Anforderungen hinwirken. So ist u. a. sicherzustellen, dass die Aufgabenbereiche der Verwaltung und der Statistik getrennt bleiben. Weiter müssen differenzierte Rollen- und Berechtigungskonzepte sicherstellen, dass Zugriffe auf Datenbestände nur durch konkret zuständige Beschäftigte und nur im notwendigen Umfang erfolgen. Der Landesbeauftragte wird die Umsetzung weiter begleiten. Es gilt zu verhindern, dass zentralisierte Datenbestände zu einem Fundus führen, der die Gefahr eines gläsernen Schülers begründet.

9.2.4 Medienkompetenz

Auch in diesem Berichtszeitraum hat sich der Landesbeauftragte in vielfältiger Weise für die Stärkung der Medienkompetenz und des Datenschutzbewusstseins insbesondere von Schülerinnen und Schülern engagiert (vgl. Nr. 1.2). Dabei ist nicht nur der verantwortungsbewusste und reflektierte Umgang mit herkömmlichen Medienangeboten in einer digitalisierten Welt zu betrachten. Medientechnik findet zunehmend auch als Lehr- und Lernmittel Verwendung. Hierbei ist neben einem sachdienlichen und zielführenden Umfang des Einsatzes auch der Aspekt der Sicherheit der verarbeiteten Daten zu berücksichtigen, was beispielsweise bei Lernplattformen von Bedeutung ist.

Nach einer Phase der Stagnation in 2015/2016 (vgl. XII. Tätigkeitsbericht, Nr. 1.4) konnten ab dem Folgejahr wieder mehr Aktivitäten seitens der Landesregierung beobachtet werden. Der Vorschlag des Landesbeauftragten für eine Kooperationsvereinbarung, angelehnt an Vorbilder in anderen Ländern, stieß im Bildungsministerium zunächst auf Aufgeschlossenheit, dann aber auf freundliches Desinteresse mit Blick auf die „Zusammenarbeit“ in der Landesarbeitsgemeinschaft „Medienbildung/Medienkompetenz“. Diese Arbeitsgruppe, in der der Landesbeauftragte Mitglied ist (vgl. LT-Drs. 7/2648), tagte im Jahr 2017 nur einmal. Erst ab dem Jahr 2018 nutzt das Bildungsministerium das Gremium wieder intensiver. Stärker in den Fokus rücken auch wieder Themen des außerschulischen Bereichs, etwa im Zusammenhang mit dem Landesprogramm „Bildung: elementar – Bildung von Anfang an“.

Besondere Aktivitäten auf dem Gebiet der Medienkompetenzvermittlung nimmt die Medienanstalt Sachsen-Anhalt wahr. Dies gilt nicht nur für den repressiven Jugendmedienschutz, etwa gemäß Jugendmedienschutz-Staatsvertrag, sondern zumal für den präventiven Jugendmedienschutz (vgl. den Bericht in LT-Drs. 7/2945) und die Unterstützung der o. a. Landesarbeitsgemeinschaft mittels des Netzwerks Medienkompetenz.

Infolge der Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“ vom Dezember 2016 entwickelte das Bildungsministerium im Frühsommer 2017 einen Entwurf eines Leitfadens bzw. Landeskonzeptes „Bildung in der digitalen Welt durch den Einsatz digitaler Medien und Werkzeuge an den Schulen des Landes Sachsen-Anhalt“ mit Angaben zu Lehrplanvorgaben, Wahlpflichtkursen, IKT-Infrastruktur und Landesbildungsserver. Außerdem werden Fachlehrpläne fortgeschrieben und Fortbildungsangebote für Lehrkräfte überarbeitet. Der fachintegrative Ansatz von digitalen Medien bzw. der Querschnittsansatz von Medienbildung gilt fort. Ein Ergänzungsstudiengang „Neues Lernen mit und über Medien – Medienbildung“ an der Universität Halle kam noch nicht zustande.

Der Landesbeauftragte kommentierte dieses Landeskonzept und forderte eine stärkere Verbindlichkeit und Nachhaltigkeit der Maßnahmen. So sollten die Erwartungen an die Kompetenzen der Schülerinnen und Schüler mit den Fortschreibungen der Fachlehrpläne und der Erarbeitung von Medienbildungskonzepten durch die Schulen zeitlich abgestimmt sein. Anfang 2018 hatte noch immer nicht jeder Landkreis einen medienpädagogischen Berater. Der Landesbeauftragte wird für diesen Adressatenkreis erneut eine datenschutzrechtliche Fortbildung, mit Schwerpunkt DS-GVO, durchführen.

Das Landeskonzept – die Endfassung wird für September 2018 erwartet – ist auch Teil der von der Landesregierung im Dezember 2017 beschlossenen Digitalen Agenda. Deutlich bleibt – worauf der Landesbeauftragte besonderen Wert legt – die Verbindung von IKT-Ausstattung, Pädagogik und Medienbildung; digitale Kompetenz ist mehr als Lernen mit Technik. Insofern reicht es nicht aus, die informatische Bildung im Rahmen der MINT-Fächer zu verstärken; auch wenn gerade die Wirtschaft Schulabgänger benötigt, die breite IT-Kenntnisse mitbringen. Vielmehr ist das Lernen über Technik bzw. die allgemeine Medienbildung im Fächerkanon vorzusehen; dies soll in Sachsen-Anhalt mit einer querschnittsmäßigen Verankerung in der Breite aller Fächer erfolgen.

Das Prinzip der Verbindung von Medienbildung und IKT-Ausstattung gilt auch für eine IKT-Förderrichtlinie des Bildungsministeriums von 2017 und zumal für den weiterhin angestrebten Digitalpakt des Bundes mit den Ländern, der aber wohl erst ab 2019 Realität werden kann. Dabei geht es in Sachsen-Anhalt vor allem um die Breitbandanbindung für die Schulen; diese soll, und das ist ein ambitioniertes Vorhaben, schon im Jahr 2020 abgeschlossen sein. Das Bildungsministerium beabsichtigt, zusammen mit dem Ministerium der Finanzen, die Rahmenempfehlung zur IT-Ausstattung von Schulen zu überarbeiten und damit das Landeskonzept „Lernen, Lehren, Managen 2.0“ von 2015 zu ersetzen. Ein kritischer, noch zu bewertender Punkt betrifft den Einsatz privater mobiler Geräte zur Unterstützung des Unterrichts.

Der Landesbeauftragte hat im Übrigen an verschiedenen Veranstaltungen auf dem Gebiet der Medienkompetenzvermittlung teilgenommen. Insbesondere sind hier im Jahre 2016 der Workshop „Schule in der digitalen Welt“, der 1. Tag der Medienkompetenz Sachsen-Anhalt, und für 2017 die 4. Netzwerktagung Medienkompetenz Sachsen-Anhalt und für beide Jahre die Vorlesungsreihe an der Hochschule Merseburg zur „Rolle und Funktion(en) von Medien in der Gesellschaft“ zu nennen.

Deutschlandweit erfolgt kontinuierlich ein thematischer Austausch im Arbeitskreis Datenschutz-/Medienkompetenz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

Zur Stärkung der Medienkompetenz und des Datenschutzbewusstseins ist auch weiterhin eine vernetzte Aufgabenwahrnehmung der verantwortlichen Stellen sinnvoll. Für eine wirksame Vermittlung von mehr Medienkompetenz sind verbindliche, nachhaltige Konzepte und Maßnahmen unabdingbar.

9.2.5 Bildungspartnerschaft mit Microsoft

Die praktische Umsetzung digitaler Bildung ist seit vielen Jahren Gegenstand von Planungen und Projekten. Das Ministerium der Finanzen überraschte im März 2015 mit einem „Letter of Intent“ zur Bildungspartnerschaft mit der Microsoft Deutschland GmbH. Ziel war die Schaffung infrastruktureller Voraussetzungen für die IT-Anbindung und IT-Ausstattung in Schulen (vgl. hierzu auch XII. Tätigkeitsbericht, Nr. 1.4). Der Landtag hat sodann die Landesregierung mit einem Beschluss vom 15. Oktober 2015 (LT-Drs. 6/4491) gebeten, auf der Grundlage der Konzeption „Lernen, Lehren, Managen 2.0“ des Ministeriums für Bildung die erforderlichen Maßnahmen zur Umsetzung vorzunehmen. Diese Konzeption beschreibt den zentral gesteuerten, strukturierten und zielgerichteten Einsatz der Informations- und Kommunikationstechnologie (IKT) zur Stärkung des individuellen Bildungserfolgs und den effektiven Einsatz von Personalressourcen. Die Leistungen im Rahmen der Bildungspartnerschaft sollten den Schulen zur freiwilligen Nutzung angeboten werden.

Neben Beratungsleistungen von Microsoft wurden drei Beschaffungsvorhaben im Zusammenhang mit dem Programmpaket Office 365 vorgesehen. Beabsichtigt waren der Abschluss eines Volumenlizenzvertrages, die Regelung der Lizenzverwaltung und die Ausgestaltung der individuellen Berechtigungsverwaltung. Im Rahmen der individuellen Berechtigungsverwaltung sollten Schülerinnen, Schüler und Lehrkräfte die Gelegenheit erhalten, Office 365 ProPlus auf bis zu 15 Geräten kostenfrei nutzen zu können. Für die Speicherung der Daten beabsichtigte das Ministerium der Finanzen, die sog. „Microsoft Cloud Deutschland“ zu nutzen, bei der T-Systems als Treuhänder letztlich die Zugangsverwaltung wahrnimmt (s. Nr. 4.12).

Der Landesbeauftragte war an mehreren Gesprächen des Ministeriums der Finanzen mit dem Ministerium für Bildung und Microsoft beteiligt. Hierbei wurde auf den Aspekt der Trennung der Daten aus dem pädagogischen Bereich vom Verwaltungsbereich hingewiesen. Erörtert wurde weiter, wie und auf welcher Rechtsgrundlage die Trennung unterschiedlicher Aufgabenbereiche und Benutzerrollen im pädagogischen Bereich und ein Identitäts- und Zugangskonzept im Zusammenhang mit einem zentralen Verzeichnisdienst zu realisieren sind.

In den Gesprächen hat Microsoft Überlegungen zu einem Prozess vorgestellt, der es Schulen auf standardisierte Weise ermöglichen soll, dem sog. Education Desktop als schulrelevantes Programmpaket beizutreten. Die Anmeldung könne über eine Verknüpfung von eigenen Verzeichnisdiensten, wie dem zentralen Verzeichnisdienst des Landes Sachsen-Anhalt oder dem einer Schule im Land, mit dem Verzeichnisdienst in der Microsoft Cloud erfolgen. Office 365 benötige jedenfalls eine Identifizierungsinformation der Benutzer.

Für den Schulbetrieb wären dann zwei Authentifizierungsprozesse erforderlich. Zum einen die Anmeldung am PC mit lokalem Konto bei der Schule oder beim Land und zum anderen die Anmeldung bei Office 365 mit einem Konto der Microsoft Cloud. Mit dem lokalen Konto werde die Anmeldung bei der Microsoft Cloud verknüpft und der Nutzer könne durchgehend in beiden Konten arbeiten. Was der Nutzer an privaten Informationen oder Dokumenten in die Microsoft Cloud überträgt, sei ihm persönlich überlassen.

Das Bildungsministerium strebte eine pseudonyme Kennung bei der Microsoft Cloud an, sodass Office 365 für Schüler nutzbar würde, ohne personenbezogene Daten preisgeben zu müssen. Das lokale Konto bei der Schule bzw. beim Land enthielte dann die Identitätsdaten der Schüler. Diese personenbezogenen Angaben sollen jedoch nicht in die Microsoft Cloud übertragen werden.

Die Nutzung von Office 365 würde auf Antrag freigeschaltet werden, indem die beiden Konten verknüpft werden würden. Das hieße, im Konto der Microsoft Cloud würde eine Information zu dem lokalen Konto beim Land oder einer Schule im Land, welches zur Nutzung von Office 365 berechtigt, hinterlegt werden. Im lokalen Konto bei der Schule oder beim Land würde die Kennung des entsprechenden Kontos in der Microsoft Cloud hinterlegt werden.

Bei der anstehenden Digitalisierung des Bildungsprozesses und der bisherigen Fokussierung der Landesregierung auf Microsoft darf nicht vernachlässigt werden, dass Microsoft nur einer der Anbieter ist. Ein weiteres Beispiel wäre das Projekt der Schul-Cloud des Hasso-Plattner-Instituts in Potsdam, worüber auch digitale Lehrinhalte zur Verfügung gestellt werden sollen. Auch sollte nicht aus dem Auge verloren werden, dass das Landesinstitut für Schulqualität und Lehrerbildung in Halle ebenfalls umfangreiche digitale Angebote zur Verfügung stellt, die schon schulfachlich geprüfte Materialien enthalten.

Ob und wie die Bildungspartnerschaft mit Microsoft fortgeführt wird, ist offen. Weiterhin steht die „Microsoft Cloud Deutschland“ noch auf dem datenschutzrechtlichen Prüfstand. Der Landesbeauftragte wird die Angelegenheit weiter begleiten.

9.2.6 Umsetzung des Berufsorientierungsprogramms des Bundes

Durch eine Eingabe wurde der Landesbeauftragte auf die Umsetzung des durch Mittel des zuständigen Bundesministeriums geförderten Berufsorientierungsprogramms (BOP) aufmerksam. Mit Hilfe der Maßnahmen nach dem BOP sollen zur Förderung des Übergangs von der Schule in den Beruf Kompetenzen festgestellt und Potentiale entdeckt werden, die die Berufswahlentscheidung unterstützen können. Das Projekt ist eingebettet in schulische berufsorientierte Lehrpläne und ist reguläre Schulveranstaltung. Schulen vereinbaren dazu die Umsetzung des Programms mit freien Bildungsträgern. Deren Sozialpädagogen führen mit den Schülerinnen und Schülern entsprechende Analysen durch, für die das Bundesministerium detaillierte Qualitätsstandards vorgibt.

Im konkreten Fall wurde gegenüber den Schülerinnen und Schüler ein Interviewleitfaden verwandt, in dem der Stichpunkt „Gegengeschlechtliche Kontakte“ mit der Frage nach Freund bzw. Freundin und der Dauer der Freundschaft abgefragt wurde. Enge Freundschaften waren im Stichpunkt zuvor bereits abgefragt worden. Wenn man davon ausgeht, dass diese Fragebögen in der 7. Klasse, 2. Halbjahr, bzw. der 8. Klasse Anwendung finden sollen, ist von einem Alter der Adressaten zwischen 12 und 15 Jahren auszugehen. Angesichts der konkreten Entwicklungssituation dieser Altersgruppe können Fragen zu sog. gegengeschlechtlichen Kontakten, insbesondere, wenn Freundschaften bereits zuvor abgefragt worden sind, durchaus falsch verstanden werden. Wie diese Fragestellungen mit der Eruierung von methodischen, personalen, sozialen und fachlichen Kompetenzen im Zusammenhang stehen, war nicht ersichtlich. Vielmehr bestand die Gefahr, dass Jugendliche, die davon ausge-

hen, sich im Rahmen der Schulpflichtveranstaltung beteiligen zu müssen, nicht erforderliche, höchst persönliche Informationen preisgeben würden. Derartige Fragestellungen erschienen daher höchst bedenklich.

Auf Nachfrage verwies die Schule auf den Kooperationsvertrag mit dem Bildungsträger. Ergänzend wurde auf weitere Nachfrage erklärt, dass es auch bei Potentialanalysen „überhaupt keine Pflicht ist“, entsprechende Angaben zu machen. Der Bildungsträger verwies auf eine Zertifizierung (allerdings lediglich zum internen Sicherheits-Management) und auf die Nutzung eines anerkannten Verfahrens. Die Angaben seien in jedem Falle freiwillig. Ausführungen dazu, wie Schülerinnen und Schüler dieser Altersklasse in Bezug auf eine Schulpflichtveranstaltung erkennen können, dass die Beantwortung von Fragen im Rahmen von Potentialanalysen freigestellt ist, wurden weder von Seiten der Schule noch von Seiten des Bildungsträgers gemacht. Die Schule hat lediglich in einer dritten Stellungnahme behauptet, die Schülerinnen und Schüler wären auf die Freiwilligkeit hingewiesen worden. Wer dies in welcher Form gemacht haben soll, blieb offen, ebenso ob diese Hinweise von der Schulleitung vorgegeben waren und deutlich und regelmäßig erfolgten. Mangels konkreter Hinweise bestand die Befürchtung, dass die Freiwilligkeit tatsächlich vor Ort zumeist nicht bzw. nicht hinreichend kommuniziert wurde.

Das Bundesministerium für Bildung und Forschung hat auf kritischen Hinweis des Landesbeauftragten hin mitgeteilt, dass das Bundesinstitut für Berufsbildung der Angelegenheit nachgegangen sei. Der Interviewleitfaden sei für die Altersgruppe nicht geeignet und dürfe künftig nicht mehr verwendet werden. Die Teilnahme an Potentialanalysen sei zwar grundsätzlich verbindlich, wenn man an den Werkstatttagen des Projekts teilnehmen wolle. Dennoch sei es für Schülerinnen und Schüler selbstverständlich möglich, auf einzelne Fragen keine Antwort zu geben, etwa, wenn die Antwort Einzelnen peinlich erscheine.

Die Umsetzung solcher Projekte erfolgt in der Verantwortung des jeweiligen Bildungsträgers. Auf Seiten der Schulverwaltung liegt aber die Verantwortung darin, zu Datenerhebungen im Rahmen pflichtiger Schulveranstaltungen darüber zu informieren, welche Daten angabepflichtig bzw. freiwillig sind. Zumindest muss vor der Teilnahme klar und deutlich bewusstgemacht werden, dass die Schülerinnen und Schüler auf einzelne Fragen/Fragenkomplexe – ohne Nachteile – nicht antworten müssen, wenn sie das nicht möchten. Das Bildungsministerium des Landes ist mehrfach auf die Angelegenheit angesprochen worden, reagierte bisher jedoch noch nicht.

9.2.7 Berufsorientierungsprogramm des Landes

Das Bildungsministerium informierte den Landesbeauftragten über den vorgesehenen landesweiten Einsatz eines Programms zur Berufsorientierung für Schülerinnen und Schüler. Aufbauend auf bisherigen Modulen zur Motivation und Berufsorientierung sollte künftig ein computergestütztes System BRAFO-KE (BRAFO – Berufswahl Richtig Angehen Frühzeitig Orientieren; KE – Kompetenz-Erkundung) verwendet werden. Dies diene u. a. der Homogenität und Vergleichbarkeit der Ergebnisse. Am ersten Tag des Programms wird über ein internetbasiertes Formular eine Selbsteinschätzung erhoben (Fragebogen, Farbreaktionstest, Einzelvergleichsverfahren) und in einer zentralen Datenbank gespeichert. Vom zweiten bis fünften Tag werden in

vier Lebenswelten aus verschiedenen Tätigkeitsfeldern Aufgaben zur Wahl gestellt. Die Ausführung der Aufgaben wird von speziell geschultem Personal auf Kompetenzskalen bewertet. Am Ende erfolgt eine Auswertung mit Empfehlung für eine Lebenswelt durch Sozialpädagogen unter Verwendung der systematischen Einordnungen und Darstellungen. Alle Zwischenergebnisse und die Auswerteergebnisse werden ebenfalls in der zentralen Datenbank gespeichert.

Der Landesbeauftragte hatte Gelegenheit, in Beratungen auf wesentliche datenschutzrechtliche Aspekte für die Umsetzung hinzuweisen. Vorrangig war von Bedeutung, dass den Schülerinnen und Schülern bei der Teilnahme bewusstgemacht wird, dass sie nicht verpflichtet sind, jegliche Fragen zu beantworten, gerade wenn ihnen einzelne Antworten ggf. unangenehm oder peinlich sind. Insoweit bestand in den Beratungen grundsätzlich Übereinstimmung. Es sollte daher auch in technischer Hinsicht versucht werden zu gewährleisten, dass einzelne Angaben ausgelassen werden können (zur Diskussion standen Fehleingaben bzw. ein „Überspringen“-Button). Zudem sollte eine entsprechende Information im Elternbrief aufgenommen werden; ohnehin musste das Einverständnis der Eltern zur Teilnahme am Projekt vorliegen.

Weiter wurde dargelegt, dass die Anwendung eines Farbreaktionstestes als weiteres Indiz zur Sicherung der Ergebnisqualität aus datenschutzrechtlicher Sicht höchst bedenklich ist. Die Probanden sollten dabei so schnell wie möglich durch Tastendruck auf die Farbeigenschaft eines semantischen Reizes reagieren. Dabei werden teilweise Worte präsentiert, die einen Bezug zu einer Lebenswelt haben. Da Menschen schneller Wörter lesen können als Eigenschaften benennen, wird bei bekannten Begriffen unterbewusst bzw. automatisch ein mentaler Prozess ausgelöst, der die Eigenschaftsangabe verzögert. Dies gebe Aufschluss über die Stärke eines assoziativen Netzwerks. Hierbei handelt es sich um ein Verfahren, das als psychologische Eignungsdiagnostik angewendet wird, u. a. für Fälle von hirnorganischen Störungen, Psychosen, Altersabbau und Legasthenie. Dies ist für die Erkundung von Schülerkompetenzen unangemessen. Schüler können nicht mehr selbstbestimmt gegenüber dem Staat bzw. den von ihm Beauftragten agieren. Dies ist ein unverhältnismäßiger Eingriff in die Persönlichkeitsrechte. Auf den Einsatz dieses Tests wurde daher verzichtet.

Die abschließende Bewertung sollte auf Basis nachvollziehbarer, transparenter Ergebnisse und nicht nur aufgrund einer maschinellen Entscheidung erfolgen. Hierzu standen spezialisierte Lehrkräfte zur Verfügung, die entsprechende Kompetenzbewertungen nach standardisierten Kriterien vornahmen.

Auch die rechtliche Ausgestaltung für die Datenverarbeitungen wurde erörtert. Es war zunächst vorgesehen, dass das Ministerium für Bildung die zentrale Datenspeicherung als verantwortliche Stelle wahrnimmt. Die Rechtsgrundlagen erschienen dafür aber fraglich, zumal letztlich die privaten Bildungsträger die Datenverarbeitungen vornehmen sollten. Auf die Notwendigkeit, dass Einwilligungserklärungen eindeutig den Sachverhalt abbilden müssen, wurde hingewiesen.

Ergänzend wurden auf technische Aspekte hingewiesen (Löschungskonzept, Vertraulichkeit) und Abstimmungen mit dem IT-Dienstleister, der die serverseitige Infrastruktur betreut, vorgenommen. Die angedachte Herausgabe der Ergebnisdokumente an die Sozialpädagogen als PDF-Datei wurde vom Landesbeauftragten kritisiert: Denn die Dateien sollten auf den jeweiligen Rechnern der Beschäftigten lokal ge-

speichert werden. Damit wären die im Konzept vorgesehenen umfänglichen Sicherheitsmaßnahmen der professionell organisierten zentralen IT-Infrastruktur beim Dienstleister konterkariert. Es müssten dann nämlich entsprechende Sicherheitsvorkehrungen auch in Bezug auf die einzelnen Rechner bei den Bildungsträgern und Sozialpädagogen getroffen werden, auf die die Daten als PDF exportiert werden. Es wurde daher empfohlen, den Ausdruck der Ergebnisdokumente direkt aus dem Webbrowser heraus zu ermöglichen. Dieser Empfehlung konnte allerdings nicht nachgegangen werden, da im Projekt kein Budget mehr vorhanden war, um derlei Zusatzfunktionen zu implementieren. Stattdessen werden die zu druckenden PDF-Dateien unter Verwendung generierter Kurzzeitpasswörter mit Hilfe eines sicheren Verschlüsselungsverfahrens auf den Rechnern der Beschäftigten vor dem Zugriff Unbefugter geschützt.

Zum geltend gemachten Interesse, Sachdaten für Forschungszwecke zur Verfügung zu haben, wurde schließlich empfohlen, die Informationen zu anonymisieren.

9.2.8 Informationsaustausch zwischen Schule und Ausbildungsbetrieb

Im XII. Tätigkeitsbericht (Nr. 9.2.4) hatte der Landesbeauftragte auf die Problematik eines unüberlegten Austauschs von Daten der Partner der dualen Ausbildung hingewiesen. Eine Neu-Regelung in der BbS-VO sah dann vor, dass sich die Partner zur Sicherung einer erfolgreichen Berufsausbildung gegenseitig über den Leistungsstand und das Lern- und Sozialverhalten der Auszubildenden informieren können. Soweit sich Lehrkräfte an berufsbildenden Schulen noch Gedanken machen, ob, wann und welche Schülerdaten an Ausbildungsbetriebe überhaupt übermittelt werden dürfen, ist diese Regelung wohl als Ermunterung zur Datenübermittlung zu interpretieren. Das aber wird dem Schutz der Schülerdaten und dem Persönlichkeitsrecht der Schülerinnen und Schüler nicht gerecht. Das Ministerium für Bildung hat die Hinweise im letzten Tätigkeitsbericht aufgenommen und Gelegenheit zu einer Beratung gegeben.

Dabei wurde auf Folgendes hingewiesen: Schulen sollten sich in eigener erzieherischer Verantwortung zunächst an die betroffenen Schülerinnen und Schüler und ggf. an die Erziehungsberechtigten wenden. Die Weitergabe von schulischen Daten an den Ausbildungsbetrieb als Dritten ist im Interesse des Grundrechts auf informationelle Selbstbestimmung der Schülerinnen und Schüler nur zulässig, wenn dies unerlässlich zur Gewährleistung des Bildungs- und Erziehungsauftrags der Schule ist. Die freizügige Information über Einzelnoten oder Fehlzeiten ist im Normalfall weder erforderlich noch zulässig. Vor einer Information an Ausbildungsbetriebe als Dritte sind die Interessen der Schülerinnen und Schüler sowie die (möglichen) Interessen der Ausbildungsbetriebe abzuwägen. Ob und inwieweit Einzelinformationen an den jeweiligen Ausbildungsbetrieb zur sachdienlichen Erfüllung der Aufgaben der Berufsbildenden Schule erforderlich sind, ist im Einzelfall abzuwägen. Dabei ist ein strenger Maßstab anzulegen. Zulässig sind beispielsweise schlichte Informationen zur Terminabstimmung oder zu schulischen und betrieblichen Ausbildungsinhalten. Sensiblere Informationen, deren Vorenthalten eine Gefahr für den Ausbildungsbetrieb, dessen Kunden, Dritte oder die Schülerin oder den Schüler selbst darstellen, können übermittelt werden. Ein Informationsaustausch ist auch vertretbar, wenn ein gemeinsames Einwirken auf die Schülerin oder den Schüler zur Erreichung des Ausbildungserfolges zwingend erforderlich ist.

Inzwischen verdeutlicht auch die neue Ausgestaltung des § 11 Satz 3 der BbS-VO (GVBl. LSA 2017, S. 81) den Erfolg der Beratung des Landesbeauftragten. Maßstab ist danach die Erforderlichkeit im konkreten Einzelfall in Wahrnehmung der pädagogischen Verantwortung im Interesse der Schülerin oder des Schülers zur Sicherung einer erfolgreichen Berufsausbildung. Auf einen sensibleren Umgang mit Schülerdaten ist also zu hoffen.

Die Kommunikation zwischen Schule und Ausbildungsbetrieb dient der sinnvollen Zusammenarbeit in der täglichen Praxis. Der Austausch von sensiblen Daten ist nur ausnahmsweise unter Berücksichtigung der Persönlichkeitsrechte der Schülerinnen und Schüler zulässig.

9.2.9 ESF-Förderprogramm „Schulerfolg sichern“

Mehrere Eingaben thematisierten die Datenverarbeitung im Rahmen des Projektes „Schulerfolg sichern“, das mit ESF-Fördermitteln finanziert wird. Unter Bezugnahme auf den Anhang I der EU VO 1304/2013 sollen die Fördermittelempfänger zu sog. „Mitwirkungspflichten“ angehalten werden. Dazu sollen durch die Projektträger Einwilligungserklärungen unter den Logos des Landes und der Europäischen Kommission verwendet werden. Es sollen zu einzelnen Teilnehmern sensible Daten personenbezogen eingetragen werden, z. B. Erwerbslosenhaushalt, Alleinerziehendenhaushalt, Migrationshintergrund, Behinderung des Kindes usw. . Die Daten sollen an verschiedene Stellen weitergeleitet werden (Landesverwaltungsamt, Ministerien usw.). Der Umfang der Datenerhebung und der Erhebungsaufwand wurden beklagt.

Die Vorgaben der Richtlinie „Schulerfolg sichern“, wonach die Zuwendungsempfänger u. a. gemäß dem Anhang I der VO (EU) Nr. 1304/2013 verpflichtet sind, die von der Bewilligungsbehörde im Zuwendungsbescheid abgeforderten Daten zu erheben, widersprachen nicht datenschutzrechlichen Anforderungen. Nach Art. 125 Abs. 2 lit. d VO (EU) Nr. 1303/2013 hat die Verwaltungsbehörde ein System einzurichten, in dem die für die Prüfung der ESF-geförderten Vorhaben benötigten Daten einschließlich der Angaben zu den Teilnehmern gespeichert werden. Auch Art. 5 VO (EU) Nr. 1304/2013 statuiert eine Berichtspflicht hinsichtlich teilnehmerspezifischer Output- und Ergebnisindikatoren. In Anhang I der VO (EU) Nr. 1304/2013 werden die Daten verbindlich vorgegeben. Die Datenverarbeitung durch die in die Verwendungsnachweisführung einbezogenen Behörden des Landes ist somit zur Erfüllung ihrer Aufgaben erforderlich und damit datenschutzrechtlich erlaubt (vgl. dazu § 11 Abs. 1, § 10 Abs. 1 DSG LSA). Auch für die Zuwendungsempfänger war die damit erforderliche Datenverarbeitung datenschutzrechtlich zulässig (vgl. dazu § 28 Abs. 1 Nr. 2 BDSG).

In der Stellungnahme des Ministeriums der Finanzen wurde auf die europarechtlichen Anforderungen hingewiesen, darüber hinaus werde eine Einverständniserklärung eingeholt und es bestehe keine Verpflichtung der Zuwendungsempfänger, Teilnehmende von der Förderung auszuschließen, wenn diese den Fragebogen nicht bzw. nicht vollständig ausfüllen. In technischer und organisatorischer Hinsicht wurde dargestellt, dass der personenbezogene Zugriff auf den Datenbestand nur im Ausnahmefall erfolge.

9.2.10 Lehrkräfteeinstellungsverfahren

Im August 2015 informierte das Ministerium für Bildung den Landesbeauftragten über die Absicht, ein Lehrkräfteeinstellungsverfahren einzurichten. Eine nähere Information blieb dann aus, obwohl dies gemäß § 14 Abs. 1 Satz 2 DSG LSA geboten war. Der Pressemitteilung 111/2016 vom 8. Dezember 2016 des Bildungsministeriums konnte der Landesbeauftragte sodann entnehmen, dass dieses ein elektronisches Bewerbungsverfahren für Lehrkräfte gestartet hat. Auch sei über das System ein Matchingverfahren zur Aufstellung von Ranglisten vorgesehen.

Hier besteht ggf. die Gefahr automatisierter Entscheidungen in Personalangelegenheiten. Der Landesbeauftragte bat daher mit Schreiben vom 20. Dezember 2016 um Zusendung des Verfahrensverzeichnisses und die Benennung bzw. Beschreibung der verantwortlichen Stelle(n), der Verfahrensabläufe, der zu speichernden Daten, der Zugriffsbefugnisse, der technischen Details und des Datenschutzkonzepts. Mit Schreiben vom 31. Juli 2017 erinnerte der Landesbeauftragte an die Angelegenheit. Eine weitere Erinnerung erfolgte mit Schreiben vom 23. November 2017. Im Februar 2018 wurde telefonisch an die ausstehenden Informationen erinnert. Im Juli 2018 lag noch immer keine Antwort vor. Damit wurde auch gegen die Pflicht zur Unterstützung des Landesbeauftragten gemäß § 23 Abs. 1 Satz 1 DSG LSA verstoßen.

10 Gesundheits- und Sozialwesen

10.1 Gesundheitswesen

Ein Schwerpunkt im Berichtszeitraum war wieder die Erhebung und Sammlung von Gesundheitsdaten der Versicherten durch Krankenkassen, insbesondere beim Krankengeldfallmanagement (s. Nr. 10.1.1). Dabei soll einerseits eine sachgerechte Betreuung der Versicherten gewährleistet werden, andererseits soll sichergestellt werden, dass die sensiblen medizinischen Daten zuständigkeitshalber nicht bei der Krankenkasse, sondern, soweit erforderlich, beim Medizinischen Dienst der Krankenversicherung liegen. Auch der Medizinische Dienst war in Bezug auf den Umgang mit den sensiblen Informationen zu beraten.

Ein Dauerthema ist die Elektronische Gesundheitskarte (eGK). Die Umsetzung des Projekts zieht sich, wohl wegen Verständigungsschwierigkeiten im System der selbstverwaltenden Gesundheitsversorgung und technischen Fragen, weiter hin. Aus datenschutzrechtlicher Sicht sind die sichere Anmeldung im System und die sichere Kommunikation von Interesse. Mit dem Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) wurde der Versuch unternommen, den Aufbau der grundlegenden Telematikinfrastruktur zu beschleunigen. Nicht nur die „klassischen“ Verwendungen der eGK, wie die Notfalldaten, eRezept oder der Medikationsplan, sollen künftig Standard werden, sondern z. B. auch Arztbriefe, Laborbefunde, vom Versicherten zur Verfügung gestellte Daten.

Das Thema Digitalisierung des Gesundheitswesens wird den Datenschutz zukünftig in steigendem Maß beschäftigen. Aktuelle Entwicklungen betreffen die Einführung einer elektronischen Gesundheitsakte (bei den Krankenversicherungen) und einer elektronischen Patientenakte (in Krankenhäusern). Auch wird die Telemedizin auf

Basis einer sicheren Kommunikationsinfrastruktur ein die Zukunft prägendes Thema (s. Nr. 10.1.4).

Angesichts der demographischen Entwicklung und der schwindenden Arztdichte in ländlichen Regionen bedarf es einer modernen digitalen medizinischen Versorgung. Seit vielen Jahren wird auf allen Ebenen an entsprechenden Projekten gearbeitet. Beispiele sind telemedizinische Projekte zur Schlaganfall-Akutversorgung (Kommunikation zwischen Schwerpunktklinik und Landarzt), Vernetzungen zur Palliativversorgung, Projekte zur umfassenden wohnortnahen Betreuung und Versorgung (z. B. Wundkontrolle per Video) oder zum fachkundigen Austausch in Bezug auf Menschen mit seltenen Erkrankungen. Unterstützendes Medium für solche Projekte soll die elektronische Patientenakte sein. Doppeluntersuchungen sollen vermieden und die Qualität der Versorgung verbessert werden. Big Data-Anwendungen sollen neue Diagnosemöglichkeiten eröffnen. Die Erweiterung der digitalen Gesundheitsversorgung erfährt eine Zusage der Unterstützung in der Digitalen Agenda für das Land Sachsen-Anhalt vom 19. Dezember 2017.

Diese Entwicklungen führen auch zu zunehmenden Beratungsbedarfen im Hinblick auf datenschutzkonforme Umsetzungen. Es muss in jedem Projekt sichergestellt sein, dass die Patientensouveränität gewahrt bleibt. Schon im XI. Tätigkeitsbericht wurde über den gesetzlich verbesserten Schutz der Patientenrechte informiert (s. Nr. 10.1.8, Patientenrechtegesetz). Weiterer Verbesserungsbedarf besteht. Die Patienten müssen zum Selbstmanagement befähigt werden. Sie müssen bestimmen können, wem sie welche Daten anvertrauen. Unbefugter Zugriff muss ausgeschlossen, der Zugriff kontrollierbar sein.

Werden die digitalen Datenschätze gehoben (zuhause, über Smartphone, Wearables oder Tablet), muss zudem die Spreu vom Weizen getrennt werden. Seriöse medizinische Verfahren sind von den unzähligen Apps zur Freizeitinformation zu unterscheiden. Und auch hierbei geht es nicht ohne Datenschutz (s. Nr. 10.1.5).

Grundlegende Voraussetzungen sind in jedem Projekt die Transparenz und die Einholung einer informierten Einwilligung. Weiter dürfen Patienten nicht durch systemische oder monetäre Anreize angehalten sein, mehr Daten zur Verfügung zu stellen, als für die Versorgung jeweils notwendig ist. Die Datenvolumina müssen steuerbar bleiben. Der Patient hat auch ein Recht auf Nichtwissen.

Die zunehmende digitale Optimierung der Gesundheitsversorgung darf nur unter Wahrung der Patientenhoheit einschließlich seiner informationellen Selbstbestimmung erfolgen.

10.1.1 Krankengeldfallmanagement

In seinem XII. Tätigkeitsbericht (Nr. 11.1.1) hatte der Landesbeauftragte über Feststellungen aus einer Kontrolle bei einer Krankenkasse berichtet. Dabei hatte er es besonders kritisch gesehen, dass sich umfangreiche medizinische Unterlagen von Versicherten in den Fallakten der Krankengeldfallmanager der Krankenkasse befanden. Die Unterlagen waren für die Bearbeitung des Krankengeldantrags durch die Krankenkasse nicht erforderlich, denn bei Zweifeln an der Arbeitsunfähigkeit sind die Krankenkassen verpflichtet, eine gutachtliche Stellungnahme des Medizinischen

Dienstes der Krankenversicherung (MDK) einzuholen (§ 275 Abs. 1 Nr. 3 SGB V). Die Leistungserbringer sind verpflichtet, die für eine gutachterliche Stellungnahme des MDK erforderlichen versichertenbezogenen Daten diesem unmittelbar zu übersenden (§ 276 Abs. 2 Satz 2 SGB V).

Das Prüfverfahren konnte inzwischen abgeschlossen werden. Der Landesbeauftragte konnte erreichen, dass die Krankenkasse medizinische Unterlagen nicht mehr für sich selbst anfordert und in den Krankengeldfallakten aufbewahrt. Im Rahmen örtlicher Erhebungen zu einer weiteren Prüfung stellte der Landesbeauftragte später fest, dass sich tatsächlich keine Unterlagen mehr in den Fallakten befanden, die nicht für die Bearbeitung im Rahmen des Krankengeldfallmanagements erforderlich waren. Die umfassende Umsetzung der Prüfungsergebnisse ist datenschutzrechtlich zu begrüßen.

10.1.2 Individuelle Beratung zum Krankengeld

Krankenkassen möchten die Versicherten bei der Reintegration in das Arbeitsleben unterstützen und setzen dabei auch auf eine umfassende Beratung und Unterstützung des Versicherten. Mit der Frage, ob sich die Krankenkassen dabei immer auf dem datenschutzrechtlich vorgesehenen Weg befinden, hat sich der Landesbeauftragte bereits in früheren Tätigkeitsberichten ausführlich auseinandergesetzt (s. XII. Tätigkeitsbericht, Nr. 11.1.1, 11.1.2 sowie XI. Tätigkeitsbericht, Nr. 10.1.6).

2016 prüfte der Landesbeauftragte erneut eine Krankenkasse zu der Frage, ob die Krankenkasse den ihren Versicherten nach § 44 Abs. 4 SGB V zustehenden Beratungs- und Unterstützungsanspruch datenschutzgerecht umsetzt. Dabei hat der Landesbeauftragte festgestellt, dass die Krankenkasse zwar in einer Vielzahl der Krankengeldfälle eine Einwilligung der Versicherten für die Inanspruchnahme der individuellen Beratungs- und Unterstützungsleistungen einholt, diese aber kaum zur Erhebung und Nutzung von zusätzlichen Daten nutzt. Beratungs- und Unterstützungsleistungen, die über allgemeine Beratungen hinausgehen und mit erweiterten Datenerhebungen verbunden sind, waren lediglich in einzelnen Fällen erkennbar, z. B. als Hilfe zum Ausfüllen von Rentenanträgen. Eine Pflicht zur Entgegennahme von Rentenanträgen haben die Krankenkassen allerdings schon nach § 16 SGB I.

Eine Erhebung und Speicherung im Rahmen der Beratungsbefugnis nach § 44 Abs. 4 SGB V bleibt auch weiterhin immer dann unzulässig, wenn der gesetzliche Aufgabenbereich des MDK tangiert wird. Die sich aus der gesetzlichen Regelung ergebenden erweiterten Datenerhebungsmöglichkeiten dürfen nicht dafür genutzt werden, dass Krankenkassen Daten erheben, die lediglich der MDK für seine Aufgabenerfüllung erheben darf.

Der Landesbeauftragte konnte in seiner Prüfung feststellen, dass die Krankenkasse die bestehenden Grenzen beachtet hat.

10.1.3 Datenübermittlung der Krankenkasse an das Sozialamt

Der Datenaustausch zwischen Sozialleistungsträgern ist immer wieder ein Thema, mit dem sich der Landesbeauftragte beschäftigen muss. Im Berichtszeitraum beschwerte sich eine Petentin über ihre Krankenkasse. Sie hatte einen Antrag auf Un-

terstützung bei der Anschaffung dringend notwendiger Brillengläser für ihre Tochter gestellt und dabei deren erhebliche gesundheitliche Einschränkungen, die zu schulischen Problemen führen, angegeben. Außerdem wies sie darauf hin, dass die Kosten für eine neue Brille, da sie alleinstehend sei, für sie eine erhebliche Belastung darstelle. Die Krankenkasse habe sich, so die Petentin, nicht zuständig gefühlt und den Antrag an das Sozialamt weitergeleitet, ohne sie zu unterrichten und ihre Zustimmung einzuholen. Sie sei entsetzt darüber, wie mit ihren privaten Informationen umgegangen worden sei.

Dem Vorgang war zu entnehmen, dass die Krankenkasse die Kosten für die Brille lediglich in Höhe der Festbeträge übernehmen konnte. Da die Petentin den Antrag aus finanziellen Gründen gestellt hatte, hielt sich die Krankenkasse nicht für den allein zuständigen Sozialleistungsträger, sondern leitete den Antrag auf den – den Festbetrag übersteigenden – Betrag sowie die Kosten der Entspiegelung der Brille an das Sozialamt weiter.

Rechtliche Grundlage für die Weiterleitung des Antrags war § 14 SGB IX. Träger der Sozialhilfe können als Rehabilitationsträger für Leistungen der medizinischen Rehabilitation, zu denen gem. § 26 Abs. 2 Nr. 6 SGB IX a. F. bzw. § 42 Abs. 2. Nr. 6 SGB IX n. F. auch Hilfsmittel zählen, in Betracht kommen. Stellt ein Leistungsträger fest, dass er für eine Leistung nicht oder nicht umfassend zuständig ist, leitet er gem. § 14 Abs. 1 Satz 2 SGB IX den Antrag unverzüglich dem nach seiner Auffassung zuständigen Rehabilitationsträger zu. Nach dieser Rechtsvorschrift ist für den Fall einer Weiterleitung des Antrages lediglich eine Unterrichtung des Antragstellers vorgesehen, die in diesem Fall unverzüglich durch die Krankenkasse erfolgt war. Eine Zustimmung des Antragstellers ist hingegen nicht vorgesehen.

Der Landesbeauftragte konnte in diesem Fall deshalb der Petentin mitteilen, dass sich die Krankenkasse aus datenschutzrechtlicher Sicht korrekt verhalten hatte.

10.1.4 Telemedizinprojekt

Dem Landesbeauftragten wurde ein Telemedizinprojekt zur Strukturierung eines Versorgungssystems vorgestellt. Das Ziel des Projekts bestand darin, die Sicherheit der Behandlung zu gewährleisten und die Eigenständigkeit und Lebensqualität von Patienten im Wohnumfeld zu sichern. Krankenpfleger oder Sozialarbeiter könnten mit Hilfe von mobilen Mess- und Kommunikationssystemen bei den Patienten in den Wohnungen oder in einer Einrichtung im Wohnumfeld die Erhebung aktueller Vitalparameter unterstützen, die letztlich dem behandelnden Arzt zur Verfügung stehen sollen. Für den Transfer der Daten und deren Speicherung war angedacht, dass ein Provider die datenspeichernde Plattform stellen soll und die Datenflüsse über ein sicheres Netz laufen könnten.

Der Landesbeauftragte hat das Projekt mit umfänglichen Hinweisen zu datenschutzrelevanten Aspekten unterstützt. Die Vorlage eines abschließenden Konzepts zur näheren Bewertung bleibt abzuwarten.

10.1.5 Wearables und Gesundheits-Apps

Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte medizinisch ausgerichtete Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet. Gesammelte und ausgewertete gesundheitsbezogene Daten können durchaus der persönlichen Lebensqualität dienen. Allerdings stehen den Vorteilen auch Risiken gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen ohne ausdrückliche Zustimmung der betroffenen Personen weiter. Zudem können erhebliche Sicherheitsdefizite dazu führen, dass sich auch Unbefugte Zugriff auf die Gesundheitsdaten verschaffen können. Deshalb hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6. und 7. April 2016 mit der Entschließung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ (**Anlage 1**) auf einige wichtige Gesichtspunkte hingewiesen:

Hersteller sollten den Grundsatz der Datenminimierung beachten. Datenschutzfreundliche Technologien und Voreinstellungen sind einzusetzen und Möglichkeiten zur pseudonymen oder verschlüsselten Verarbeitung einzuräumen. Eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte sollte transparent sein, möglichst einer medizinischen Behandlung dienen und auf einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung beruhen. Im Hinblick auf die rechtlichen Grundlagen und die technischen Rahmenbedingungen sieht die Datenschutzkonferenz bei diesen zahlreichen Apps im Gesundheitsbereich den Gesetzgeber in der Pflicht. Lediglich einige wenige medizinische Produkte müssen ein sog. Konformitätsbewertungsverfahren nach dem Medizinproduktegesetz durchlaufen; dieses stellt aber nur auf die Produktsicherheit und die Leistungsfähigkeit ab.

Aber auch der einzelne Anwender sollte sich genau ansehen, wem er seine gesundheitsbezogenen Daten anvertraut. So hatte das Bayerische Landesamt für Datenschutzaufsicht im Jahr 2016 mit einigen weiteren Aufsichtsbehörden sog. Wearables geprüft (Fitness-Armbänder, Smart Watches mit Gesundheitsfunktionen, Apps der Hersteller). Dabei wurden zahlreiche Datenschutzmängel bei den Fitness-Trackern festgestellt. Insbesondere war nicht transparent, was mit den eigenen Daten passiert. Teilweise werden die Nutzung zu Forschungszwecken und für Marketing und die Weitergabe an verbundene Unternehmen in den Nutzungsbedingungen zwar erwähnt, nähere Einzelheiten bleiben aber offen (s. Bayerisches Landesamt für Datenschutzaufsicht, 7. Tätigkeitsbericht, Nr. 3.11; vgl. auch Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen, 23. Datenschutz- und Informationsfreiheitsbericht 2017, Nr. 10.6).

Die Hersteller sog. Wearables sind gehalten, für Transparenz und Datenminimierung (Datenschutz durch Technikgestaltung) zu sorgen. Der Gesetzgeber ist aufgerufen, Rechtsgrundlagen und Rahmenbedingungen zu formulieren. Die Nutzer sollten sich genau ansehen, wem sie ihre Daten anvertrauen.

10.1.6 Klinisches Krebsregister Sachsen-Anhalt

Die bundesgesetzlich gebotene Einrichtung einer flächendeckenden klinischen Krebsregistrierung gem. § 65c SGB V hat der Landesbeauftragte im XII. Tätigkeitsbericht (Nr. 11.1.9) dargestellt. Umfängliche Beratungen des Ministeriums für Arbeit, Soziales und Integration auch unter Beteiligung der von der notwendigen Neuregelung betroffenen bisherigen regionalen Krebsregister gaben Gelegenheit, auf die gebotene Berücksichtigung der Persönlichkeitsrechte der betroffenen Krebskranken hinzuwirken. Sehr viele Anregungen des Landesbeauftragten wurden in das Gesetz über die Krebsregistrierung im Land Sachsen-Anhalt (Krebsregistergesetz Sachsen-Anhalt – KRG LSA; GVBl. LSA 2017, S. 173) aufgenommen.

Das Gesetz sieht vor, dass ein zentrales Landeskrebsregister in Form einer gGmbH in alleiniger Trägerschaft der Ärztekammer Sachsen-Anhalt und in Verantwortung des Landes mit den Aufgaben des § 65c SGB V beliehen wird. Zur Gewährleistung des gebotenen Schutzes der sensiblen Daten wird vorgegeben, dass das Register ein Datenschutzkonzept erstellt, in dem die Datenverarbeitung differenziert geregelt wird. Auf die Einrichtung von selbständigen, räumlich, organisatorisch und personell getrennten Vertrauens- und Registerstellen wird angesichts der geringen Größe der Einrichtung verzichtet. Es soll jedoch lediglich einem detailliert abgegrenzten Personenkreis möglich sein, auf die Identitätsdaten der Patienten (Name, Anschrift usw.) zuzugreifen. Durch technische und organisatorische Maßnahmen soll sichergestellt werden, dass Zugriffe auf diese Identitätsdaten sowie auf die medizinischen Daten nur im Rahmen der Erforderlichkeit für die konkrete Aufgabenerfüllung möglich sind. Innerhalb der IT-Infrastruktur wird somit eine logische Trennung der Datenverarbeitung nach unterschiedlichen Verarbeitungszwecken gewährleistet. Der Landesbeauftragte wird die konkrete Ausgestaltung des Datenschutzkonzeptes und seine technische Umsetzung durch die Klinische Krebsregister Sachsen-Anhalt gGmbH intensiv begleiten.

Im Rahmen des Gesetzgebungsverfahrens blieb aus datenschutzrechtlicher Sicht zu bemängeln, dass das grundsätzlich positiv zu bewertende Widerspruchsrecht gegen die Speicherung der Daten sich nicht mehr auf die Daten bezieht, die für das epidemiologische Gemeinsame Krebsregister in Berlin vorgesehen sind. Damit wird das bisher bestehende Recht auf Widerspruch gegen die Registrierung im Gemeinsamen Krebsregister abgeschafft. Dagegen gibt es beim klinischen Krebsregister ein Widerspruchsrecht, allerdings werden hierbei die Identitätsdaten gespeichert. Dies ist zwar sinnvoll, um bei weiteren Meldungen zu wissen, dass ein Widerspruch vorliegt. Eine Nutzung von Kontrollnummern (Pseudonymisierung) würde dem Ziel der Datenminimierung aber eher entsprechen. Kritisiert wurden auch Regelungen zum sehr umfangreichen Austausch von Daten unter den Krebsregistern der Länder. Auch war nicht nachvollziehbar, warum die Daten personenbezogen bis 50 Jahre nach dem Tod oder 130 Jahre nach der Geburt gespeichert bleiben müssen. Auch hier wäre eine Pseudonymisierung der Daten zu bevorzugen gewesen.

Auch in Bezug auf das epidemiologische Register gemäß dem Staatsvertrag über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen erfolgte eine Anpassung (GVBl. LSA 2017, S. 190). Es geht u. a. um die Wahrnehmung von neuen Aufgaben nach dem Bundeskrebsregisterdatengesetz, die Abstimmung mit Neuregelungen zu den klinischen Krebsregistern (Abgleich von Daten aus den Mel-

deregistern und den Leichenschauscheinen) und die Anpassung an die aktuelle Krebs-Früherkennungsrichtlinie des Gemeinsamen Bundesausschusses. Die datenschutzrechtliche Begleitung erfolgte durch die Berliner Landesbeauftragte für Datenschutz und Informationsfreiheit, die die anderen Landesbeauftragten beteiligt hatte.

10.1.7 Auswertung der Prüfung der Webshops bei Apotheken – Medikamentenbestellung mithilfe von WhatsApp

Den Landesbeauftragten erreichten bereits vor dem Berichtszeitraum einige Beschwerden, deren Gegenstand Verletzungen des Datenschutzes beim Betrieb der Webshops von Versandapotheken waren. Er entschloss sich daher, größere Versandapotheken in Sachsen-Anhalt hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften zu überprüfen. Die Überprüfung führte zu folgenden Feststellungen:

Bestellbestätigung per E-Mail

Mitunter wurden Bestellungen von Medikamenten durch die Versandapotheken mittels unverschlüsselter E-Mail bestätigt. Eine Bestellbestätigung ist zwar gemäß § 312i Abs. 1 Nr. 3 BGB erforderlich. Durch eine unverschlüsselte E-Mail ist dies aber nur dann zulässig, wenn die Bestätigungsmail keine personenbezogenen Gesundheitsdaten enthält, da die Kenntnisnahme Unberechtigter beim Versand unverschlüsselter E-Mails nicht ausgeschlossen werden kann. Sofern die Bestellbestätigung nicht verschlüsselt erfolgt, wurde den Apotheken geraten, den Kunden lediglich z. B. mitzuteilen "Ihre Bestellung vom... ist bei mir eingegangen und wird bearbeitet." Eine weitere Möglichkeit wäre, die Bestellbestätigung unmittelbar im Anschluss an den erfolgreichen Bestellvorgang unter Aufrechterhaltung der HTTPS-Verbindung im Browser anzuzeigen, sodass der Kunde sie abspeichern oder ausdrucken kann.

Berufung auf die Einwilligung in Datenschutzerklärungen

Bei einigen Versandapotheken enthielt die Datenschutzerklärung die Aussage, dass die Datenverarbeitung im Rahmen von Bestellvorgängen auf die Einwilligung der Kunden gestützt wird. Wurden personenbezogene Daten für die Begründung, Durchführung oder Beendigung von Schuldverhältnissen erhoben, verarbeitet oder genutzt, war § 28 Abs. 1 BDSG die Rechtsgrundlage. Die Berufung auf die Einwilligung täuschte hier vor, dass der Kunde Einfluss auf die Datenverarbeitung hat, diese aber tatsächlich vom abzuschließenden Geschäft abhängt. Auf die Einwilligung sollte nur dann verwiesen werden, wenn eine Datenverarbeitung nicht auf einer Erlaubnisvorschrift beruht. So war die Erhebung und Speicherung von Lieferanschriften auf der Grundlage von § 28 BDSG möglich, ein Hinweis auf die Einwilligung verwirrte hier nur.

Bonitätsabfragen

Einige AGB bzw. die Datenschutzerklärungen der Versandapotheken enthielten unklare Formulierungen zur Durchführung von Bonitätsabfragen, sodass für den Kunden nicht erkennbar war, wann diese wirklich erfolgen.

Bonitätsabfragen durften gemäß § 28 Abs. 1 Nr. 2 i. V. m. § 29 Abs. 2 Satz 1 BDSG durchgeführt werden, soweit sie zur Wahrung berechtigter Interessen der Apotheke erforderlich waren und kein Grund zu der Annahme bestand, dass das schutzwürdi-

ge Interesse des Kunden an dem Ausschluss der Verarbeitung oder Nutzung überwog.

Dies war regelmäßig nur dann gegeben, wenn es um Geschäftsabschlüsse ging, die mit einem wirtschaftlichen Risiko verbunden waren – besonders dann, wenn eine Vorleistung erbracht werden sollte, zum Beispiel beim Kauf auf Kredit, nicht aber bei sofortiger Bezahlung. Darauf sollte auch in den AGB eindeutig hingewiesen werden.

Werbung

Einige AGB enthielten ungenaue, teilweise auch falsche Ausführungen zur Datennutzung für Werbezwecke. Dazu wurde folgender Hinweis erteilt:

Datenschutzrechtlich wird bei der Nutzung von personenbezogenen Daten für Werbezwecke gem. § 7 Abs. 3 UWG zwischen Bestands- und Neukunden und zwischen Briefpost und elektronischer Post (bzw. SMS, Telefon, Telefax) unterschieden. Diese rechtlich gebotene Differenzierung muss sich auch in den AGB widerspiegeln, soweit Sie personenbezogene Daten für Werbezwecke nutzen wollen. Näheres dazu ist in dem Merkblatt „Was darf Werbung?“ zu entnehmen, welches auf der Homepage[6] des Landesbeauftragten abrufbar ist oder bei diesem bestellt werden kann.

Verschlüsselung der Webseiten

Ein Hauptproblem stellt die oft nicht durchgängige Verschlüsselung der Webseiten dar. So war bei einigen der überprüften Versandapotheken der eigentliche Online-Shop zwar verschlüsselt. Beim Kundenlogin, der Registrierung als Neukunde und der Bestellung als Gast erfolgte die Übertragung personenbezogener Daten jedoch unverschlüsselt. Auch das Kontaktformular war häufig unverschlüsselt. Das hat zur Folge, dass die Vertraulichkeit der übertragenen und i. d. R. besonders sensiblen Gesundheits- oder Bankdaten nicht gewährleistet ist, da unbefugte Dritte diese während der Übertragung zur Kenntnis nehmen können.

Gemäß § 13 Abs. 7 des Telemediengesetzes (TMG) war der Diensteanbieter verpflichtet, die geschäftsmäßig angebotenen Telemedien gegen Verletzungen des Schutzes personenbezogener Daten zu sichern. Die getroffenen Vorkehrungen mussten dem jeweiligen Stand der Technik entsprechen, z. B. Verschlüsselungsverfahren. Um eine sichere Verbindung zwischen dem Endgerät des Kunden und dem Server der Apotheke zu gewährleisten, sollte derzeit mindestens das Verschlüsselungsprotokoll Transport Layer Security (TLS) 1.2 verwendet werden (s. Nr. 4.10). Ältere TLS-Versionen sind nicht ausreichend sicher und entsprechen damit nicht mehr dem Stand der Technik.

Im Übrigen stellte die fehlende oder nicht durchgängige Verschlüsselung bei der Übertragung personenbezogener Daten eine Ordnungswidrigkeit gemäß § 16 Abs. 2 Nr. 3 TMG dar, die gemäß § 16 Abs. 3 TMG mit einer Geldbuße bis zu 50.000 € geahndet werden konnte.

---

[6] http://lsaurl.de/WasDarfWerbung

Verwendung von Webtracking-Tools

Um das Verhalten der Nutzer ihrer Webseiten zu analysieren, verwenden viele Apotheken Webtracking-Tools wie z. B. Google Analytics. Gemäß § 15 Abs. 3 TMG durften Diensteanbieter Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Dabei ist zu beachten, dass es sich bei IP-Adressen nicht um Pseudonyme, sondern personenbezogene Daten handelt (vgl. Urteil des EuGH vom 19. Oktober 2016, Az. C 582/14) und diese deshalb nur anonymisiert gespeichert werden dürfen. Auf die Verwendung von Webtracking-Tools und sein Widerspruchsrecht war der Nutzer im Rahmen der datenschutzrechtlichen Unterrichtung gemäß § 13 Abs. 1 TMG hinzuweisen.

Da Google Analytics das am häufigsten eingesetzte Webtracking-Tool ist, kommt es insbesondere auf die Aufklärung der Nutzerinnen und Nutzer in der Datenschutzerklärung über die Verarbeitung ihrer personenbezogenen Daten und Hinweise auf die Widerspruchsmöglichkeiten an. Zur Deaktivierung von Google Analytics stellt Google ein Browser-Add-on[7] zur Verfügung, auf das in der Datenschutzerklärung verlinkt werden sollte.

Es ist davon auszugehen, dass Google aufgrund der Vielzahl der angebotenen Dienste in der Lage ist, mittels Google Analytics umfangreiche Nutzerprofile auch ohne Speicherung vollständiger IP-Adressen zu erstellen. Deshalb empfiehlt der Landesbeauftragte, alternative Webtracking-Tools einzusetzen, bei denen der Webseitenbetreiber die Nutzungsdaten auf dem eigenen Server auswertet und keine Weitergabe der Daten an Dritte erfolgt.

Verwendung von sog. Social Plugins

Einige Apotheken haben auf ihren Webseiten sog. Social Plugins eingebunden (z. B. Gefällt-mir- oder Teilen-Button von Facebook). Dabei ist zu beachten, dass die direkte Einbindung von Social Plugins datenschutzrechtlich unzulässig ist, da schon beim Aufruf der Webseite Daten an Facebook & Co. übermittelt werden, ohne dass der Nutzer auf den jeweiligen Button geklickt hat und damit in die Übermittlung seiner Daten einwilligt (vgl. Nr. 5.6.2)

Medikamentenbestellung mithilfe von WhatsApp

Unabhängig von der Überprüfung der Online-Versandapotheken ist dem Landesbeauftragten bekannt geworden, dass einige Apotheken ihren Kunden den Service anbieten, Medikamente zu bestellen, indem sie ein Foto ihres Rezepts per WhatsApp versenden. Die Medikamente werden dann für den Kunden zur Abholung bereitgelegt.

Der Einsatz von WhatsApp ist datenschutzrechtlich sehr bedenklich, zumal die Rezepte auch Aufschluss über Erkrankungen geben können und somit sensible Gesundheitsdaten übermittelt werden. Der Inhalt der durch WhatsApp versandten Nachricht ist zwar durch eine Ende-zu-Ende-Verschlüsselung geschützt. Jedoch ist nicht bekannt, ob WhatsApp nicht auch verschlüsselte Daten mitlesen kann. Nicht ver-

[7] https://tools.google.com/dlpage/gaoptout?hl=de

schlüsselt und in den USA gespeichert werden jedenfalls die Metadaten (Kommunikationsteilnehmer, Zeitpunkt und Umfang der Kommunikation). Zudem hat WhatsApp Zugriff auf alle Kontakte, die im Smartphone gespeichert sind, denn das Telefonbuch wird automatisch abgeglichen. Dabei können auch personenbezogene Daten von Dritten an WhatsApp übermittelt werden, die in diese Übermittlung nicht eingewilligt haben (vgl. Nr. 5.7).

Die Feststellungen erfolgten aufgrund der alten Rechtslage, insbesondere den Regelungen des BDSG und des TMG. Seit dem 25. Mai 2018 ist jedoch die DS-GVO unmittelbar anzuwenden. Da beim Betreiben eines Webshops elektronische Kommunikationsdaten (Metadaten und Inhaltsdaten) verarbeitet werden, ist zusätzlich – nach ihrer Verabschiedung – auch die E-Privacy-Verordnung zu beachten (s. Nr. 5.1). Die Versandapotheken sowie andere Betreiber von Webshops sind aufgefordert, die Entwicklung hinsichtlich der E-Privacy-Verordnung zu beobachten und ihre elektronische Kommunikation rechtzeitig an die dann neue Rechtslage anzupassen.

10.1.8 Einsatz externer Dienstleister durch Berufsgeheimnisträger

Die Einschaltung externer Dienstleister ist infolge der Technisierung seit langem bei vielen Berufsgeheimnisträgern notwendig, da sie nicht über die notwendigen IT-Kenntnisse verfügen. Dies betrifft vor allem auch Ärzte mit ihren Praxisinformationssystemen. Datenschutzrechtlich ist die Einschaltung auf dem Wege der Datenverarbeitung im Auftrag möglich. Allerdings droht stets eine Strafbarkeit wegen Verletzung der ärztlichen Schweigepflicht (§ 203 StGB). Die Datenschutzaufsichtsbehörden hatten daher seit langem eine gesetzliche Ausgestaltung gefordert. Mit der Entschließung der Konferenz vom 15. März 2017 „Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!“ haben sie ihrer Forderung nach einer sachdienlichen gesetzlichen Regelung Ausdruck verliehen (**Anlage 12**).

Zwischenzeitlich ist durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BGBl. I 2017, S. 3618) eine Änderung von § 203 StGB erfolgt. Das Einschalten sog. mitwirkender Personen im Rahmen des Erforderlichen ist damit keine strafbewehrte Offenbarung von Patientengeheimnissen mehr. Allerdings ist zur Vermeidung von Strafbarkeit zu beachten, dass die mitwirkende Person zur Verschwiegenheit verpflichtet werden muss. Die mitwirkenden Personen unterliegen ebenfalls der strafbewehrten Schweigepflicht.

10.2 Sozialwesen

10.2.1 Anpassung des SGB an die DS-GVO

Die Anpassung des deutschen Rechts an die Vorgaben der DS-GVO macht auch vor dem Sozialgesetzbuch keinen Halt. Im Rahmen des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften (BGBl. I 2017, S. 2541) sind bereits das SGB I und das SGB X in Teilen angepasst worden. Weitestgehend wurden die bisherigen Vorschriften des SGB X zum Datenschutz übernommen. In einigen Bereichen gehen die Regelungen weiter. So sind z. B. die Vorschriften zur Ver-

wendung von Sozialdaten zu Forschungszwecken ausgeweitet worden. Zur Datenverarbeitung im Auftrag erfolgen neben einer Bezugnahme auf Art. 28 DS-GVO weitere Ausgestaltungen und auch Lockerungen. So besteht bei der Datenverarbeitung im Auftrag durch nichtöffentliche Stellen nicht mehr die Einschränkung, dass der übertragene Umfang nicht den gesamten Datenbestand des Auftraggebers umfassen darf. Weiter finden sich spezifische Regelungen zu den Informationspflichten des Verantwortlichen und zum Auskunftsrecht der betroffenen Person. Änderungen an anderen Büchern des Sozialgesetzbuchs sind geplant.

10.2.2 Prüfung von Jobcentern

Im zurückliegenden Berichtszeitraum hat der Landesbeauftragte zwei Jobcenter vor Ort nach einzelfallunabhängigen Kontrollen zu datenschutzrechtlichen Fragen beraten. Auffällig war dabei insbesondere, dass bestimmte Themen, die bereits Gegenstand früherer Tätigkeitsberichte waren, weiterhin Anlass zu Kritik gaben.

Freiwilligkeit der Angabe von Telefonnummern

Beide Jobcenter nutzten Formulare, in denen die private Telefonnummer der Antragsteller nicht als freiwillige Angabe gekennzeichnet war. Diese Feststellung hatte der Landesbeauftragte bereits in seinem X. Tätigkeitsbericht (Nr. 22.9) aufgegriffen. Offenbar scheint es weiterhin für Sozialleistungsträger schwierig zu sein, zwischen erforderlichen und „nützlichen“ Daten zu unterscheiden. Selbst wenn die Angabe einer Telefonnummer für Rückfragen hilfreich sein könnte, steht es dem Antragsteller grundsätzlich frei zu entscheiden, ob er bei Rückfragen vom Sozialleistungsträger angerufen werden möchte oder Rückfragen auf anderem Wege erfolgen sollen. Beide Jobcenter haben ihre Antragsformulare inzwischen überarbeitet.

Telefonnummern der Antragsteller gehören nicht zu den für die Leistungsentscheidung erforderlichen Daten. Die Angabe der Telefonnummer ist in Formularen deshalb als „freiwillige Angabe“ zu kennzeichnen.

Löschung von Sozialdaten

Beide Jobcenter verfügten nicht über ein Löschungskonzept. Sie waren nicht dafür sensibilisiert, dass Sozialleistungsträger die Verantwortung dafür tragen, Sozialdaten zu löschen, wenn deren Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist (§ 84 Abs. 2 Satz 2 SGB X). Ein Jobcenter gab an, erst zum 1. Januar 2012 gegründet worden zu sein; die Aufbewahrungsfristen seien noch nicht abgelaufen und deshalb sei eine Löschung bisher entbehrlich gewesen. Die Prüfung eines Einzelfalls ergab hier jedoch, dass Arbeitsunfähigkeitszeiten aus mehr als zwanzig Jahre zurückliegenden Zeiträumen gespeichert wurden. Auf Nachfrage konnte das Jobcenter die Erforderlichkeit nicht begründen.

Um die rechtliche Verpflichtung zur Löschung von Sozialdaten zu erfüllen, empfiehlt es sich, ein Löschungskonzept zu entwickeln. Darin wird festgelegt, wie die datenschutzrechtlichen Pflichten zur Löschung von Sozialdaten umgesetzt werden. Die „Leitlinie zur Entwicklung eines Löschungskonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ des Deutschen Instituts für Normung e. V., das als Informationsmaterial auf den Internetseiten der Bundesbeauftragten für den Daten-

schutz und die Informationsfreiheit abrufbar ist, bietet hilfreiche Hinweise für die Erstellung eines Löschungskonzeptes.

Sozialleistungsträger dürfen Daten nur so lange speichern, wie diese zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich sind. Nicht mehr erforderliche Daten sind grundsätzlich zu löschen.

Hausbesuche

Die Durchführung von Hausbesuchen (s. ausführlich XII. Tätigkeitsbericht, Nr. 11.2.2) war zwar in den beiden Jobcentern durch Dienst- bzw. Organisationsanweisungen geregelt. Beide Jobcenter haben die besonderen Umstände beschrieben, die die Durchführung eines unangekündigten Hausbesuchs ausnahmsweise rechtfertigen würden. Die Dokumentation unterblieb jedoch in den geprüften Einzelfallakten. Somit war nicht feststellbar, ob für diesen außerordentlich starken Grundrechtseingriff, den ein – insbesondere unangekündigter – Hausbesuch darstellt, eine besondere Rechtfertigung gegeben war.

Hausbesuche stellen einen außerordentlich starken Grundrechtseingriff dar und sind deshalb nur unter Beachtung des Grundsatzes der Verhältnismäßigkeit – nach Ausschöpfung anderer Mittel zur Sachverhaltsaufklärung – zulässig. Insbesondere bei unangekündigten Hausbesuchen sind die Jobcenter gehalten, die Gründe für den Hausbesuch sorgfältig zu prüfen und zu dokumentieren.

10.2.3 Bestätigungen Dritter auf Anträgen

Dass Sozialdaten vorrangig beim Betroffenen zu erheben sind, ist trotz wiederkehrender Hinweise in früheren Tätigkeitsberichten (X. Tätigkeitsbericht Nr. 22.2, XII. Tätigkeitsbericht Nr. 11.2.5) immer noch nicht allen Sozialleistungsbehörden bewusst. So musste sich der Landesbeauftragte im Berichtszeitraum mit der Frage beschäftigen, ob Dritte Angaben der Antragsteller im Antragsformular bestätigen müssen. Eine Beschwerdeführerin gab an, auf Formularen des Jobcenters müsse der Versicherungsvertreter die Angaben des Antragstellers zu bestehenden Versicherungen grundsätzlich bestätigen. Das Antragsformular enthalte das Logo des Jobcenters, sodass dem Versicherungsvertreter und damit auch der Versicherung dadurch der Sozialleistungsbezug bekannt werde. Sie fragte, ob dies wirklich erforderlich sei und ob nicht die Vorlage des Versicherungsscheins genüge.

Der Landesbeauftragte wies das Jobcenter darauf hin, dass jeder einen Anspruch darauf hat, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis, § 35 Abs. 1 Satz 1 SGB I). Als Form der Verarbeitung gilt auch die Übermittlung von Sozialdaten. Die Tatsache des Bezugs von Sozialleistungen ist ebenfalls ein schützenswertes Sozialdatum.

In seiner Stellungnahme gab das Jobcenter an, dass für die Prüfung der Verwertbarkeit von Lebensversicherungen die Vorlage des Versicherungsscheines nicht ausreiche. So seien auch Angaben zum Rückkaufswert der Versicherung, zur Höhe der gezahlten Beiträge, zur Höhe des Auszahlbetrages zum Antragszeitpunkt sowie zu einem unwiderruflich vereinbarten Verwertungsausschluss erforderlich. Diese Anga-

ben würden sich nicht aus dem Versicherungsvertrag ergeben. Das Formular werde verwendet, um die erforderlichen Daten gebündelt vollständig zu erheben, ohne dass der Antragsteller eine Vielzahl verschiedener Dokumente, die vorher stichtagsbezogen zu aktualisieren wären, beibringen müsse. Der überwiegende Teil der Antragsteller würde dies als Erleichterung ansehen. Darüber hinaus seien Versicherungen nach § 60 Abs. 2 Satz 1 SGB II verpflichtet, dem Jobcenter Auskünfte über Vermögenswerte und jeweils damit in Zusammenhang stehendes Vermögen oder Einkommen des Antragstellers zu erteilen. Damit sei die Verwendung des Logos des Jobcenters gerechtfertigt.

Der Landesbeauftragte erläuterte dem Jobcenter, dass es grundsätzlich ausreichen dürfte, dem Antragsteller ein neutrales, nicht mit dem Logo des Jobcenters versehenes Formular mitzugeben, damit dieser – sofern er die Angaben nicht selbst von seiner Versicherung erfragen und Nachweise beibringen möchte – das Formular seiner Versicherung vorlegen kann. Einer Offenbarung, für welche Stelle das Formular benötigt wird, bedarf es hierfür nicht.

Davon abzugrenzen sind hingegen sicher solche Fälle, in denen das Jobcenter die Angaben von der Versicherung nach § 60 Abs. 2 Satz 1 SGB II anfordern muss, weil z. B. der Antragsteller weder selbst noch von seiner Versicherung ausgefüllte Unterlagen beibringt. Hier dürfte wegen der mangelnden Mitwirkung des Antragstellers die Offenbarung des Sozialleistungsbezugs erforderlich sein, um den Versicherer auf seine gesetzliche Mitwirkungspflicht hinweisen zu können.

Das Jobcenter hat sich der Argumentation des Landesbeauftragten angeschlossen. Es hat das Antragsformular nun so gestaltet, dass sich die Antragsteller die erforderlichen Angaben der Versicherung durch einen Vertreter in einem abzutrennenden Teil des Formulars, welches neutral gestaltet ist, bestätigen lassen können. Dadurch ist sichergestellt, dass der Versicherung der Sozialleistungsbezug nicht mehr offenbart wird.

Auch beim Sozialleistungsbezug gilt der Ersterhebungsgrundsatz nach § 67a Abs. 2 Satz 1 SGB X. Es ist grundsätzlich nicht erforderlich, Antragsformulare so zu gestalten, dass Dritten zwangsläufig der Umstand eines Sozialleistungsverfahrens bekannt wird.

10.2.4 Angaben zum „Erscheinungsbild“

Erfolgreiche Arbeitsvermittlung setzt auch voraus, dass das Jobcenter Daten zu Vermittlungshemmnissen oder individuellen Hilfebedarfen erhebt und speichert, um durch passgenaue Angebote Vermittlungshindernisse abbauen zu können. Doch wie ist es mit Informationen zum Erscheinungsbild und Auftreten des Betroffenen?

Ein Petent beschwerte sich beim Landesbeauftragten, dass ein Jobcenter Daten zu seinem Aussehen ohne seine Einwilligung gespeichert habe.

Das um Stellungnahme gebetene Jobcenter teilte mit, zur Aufgabe der zuständigen Jobcentermitarbeiter gehöre es, die Situation des Leistungsberechtigten zu analysieren und Vermittlungs- und Integrationsstrategien zu entwickeln. Hierzu müssten die einzelfallbezogenen Problemlagen jedes einzelnen erwerbsfähigen Leistungsberechtigten erhoben werden, welche als Grundlage zur Erstellung einer individuellen In-

tegration- und Hilfeplanung dienen. Angaben zu persönlichen Eigenschaften oder beruflichen Schlüsselkompetenzen sowie Angaben zur Erwerbsfähigkeit und psychische, physische und intellektuelle Einschränkungen oder Suchterkrankungen werden unter Beachtung der datenschutzrechtlichen Vorschriften erhoben. Die Mitarbeiter behandeln diese Daten streng vertraulich. Vermerke können nur von hierzu berechtigten Personen gelesen werden; eine Weitergabe dieser Daten an Dritte erfolge nicht.

In mehreren Gesprächen seien bei dem Petenten Anzeichen für vorherigen Alkoholkonsum (Alkoholgeruch, gerötete Augen) festgestellt worden. Dies sei dokumentiert worden, um bei wiederholten Anzeichen eine mögliche Suchtproblematik besprechen zu können. Gemäß § 16a SGB II sei es im Rahmen der kommunalen Eingliederungsleistungen dann möglich, Hilfestellungen wie das Aufsuchen einer Suchtberatungsstelle anzubieten.

Aus datenschutzrechtlicher Sicht ist ein Erfassen von individuellen Kompetenzmerkmalen oder Problemlagen nur in engen Grenzen zulässig (§ 67a Abs. 1 Satz 1 SGB X). Dies setzt voraus, dass eine pauschale Bewertung wie anhand von Schulnoten oder allgemeinen Merkmalen unterbleibt (vgl. Nr. 10.2.5). Es können jedoch Feststellungen bei Beratungsterminen erforderlich sein, um mit entsprechenden Maßnahmen Vermittlungshindernisse abzubauen. Dazu können tatsächliche Feststellungen notiert und in der Akte dokumentiert werden. Da den Eintragungen tatsächliche Beobachtungen der Mitarbeiter zugrunde lagen und die Erhebung für die Aufgabenerfüllung des Jobcenters, z. B. für die Hilfeplanung, erforderlich war, war das Erheben und Speichern der tatsächlichen Feststellungen datenschutzrechtlich zulässig.

Sollten Sozialdaten unrichtig sein, könnte ein Berichtigungsanspruch bestehen (§ 84 Abs. 1 Satz 1 SGB X). Wird die Richtigkeit der Sozialdaten bestritten, es lässt sich aber weder die Richtigkeit noch die Unrichtigkeit der Sozialdaten feststellen, sind die Daten nicht im Zweifel zu berichtigen oder zu löschen, sondern es ist in geeigneter Weise festzuhalten, dass die Richtigkeit bezweifelt wird. Dies kann insbesondere durch einen schriftlichen Vermerk oder bei automatisierten Dateien durch eine bei den Daten hinterlegte Zusatzinformation erfolgen.

10.2.5 Vermittlungsprogramm im Jobcenter

Ein vom Landesbeauftragten besuchtes Jobcenter verwendete für die Vermittlungsaufgaben bereits ein Softwareprogramm. Die Verarbeitung der Sozialdaten wurde in einer Vielzahl von Masken in Menüs und Untermenüs dargestellt.

In den Menüs wurden zunächst die grundlegenden Informationen zum einzelnen Vermittlungsfall aufgeführt. Zum Bewerberprofil fanden sich Angaben für die Arbeitsplatzsuche (Vermittlungsanforderungen zur Person, wie ABM, Reha, möglicher Arbeitsumfang, Vollerwerb) sowie für Berufswünsche und zum Aspekt der Berufsentfremdung gem. § 81 Abs. 2 Nr. 1 SGB III. Erfasst wurden auch Qualifikationsaspekte, wie Schulabschluss und Führerschein (einschließlich Mobilitätsangaben: keine, regional, überregional; Führerscheinklasse, Fahrzeug vorhanden). Fachspezifische Kenntnisse (beispielsweise für den Berufsbereich Callcenter: u. a. die Einzelkompetenzen im Bereich Telemarketing, Telefoninterview, Fernsprechauskunft) und Zertifikate für die einzelnen Berufsgruppen (wie z. B. Schweißerprüfungen, mit verschie-

denen Untergruppierungen und Gültigkeitsdaten) wurden ebenso gespeichert wie Sprachkenntnisse zu Mutter- und Fremdsprache sowie zum Sprachniveau (Schulkenntnisse, Grundkenntnisse, erweiterte Kenntnisse, Verhandlungssicherheit).

Im Bereich Profiling konnten die Kompetenzebenen Methodenkompetenz, Aktivitäts- und Umsetzungskompetenz, sozial-kommunikative Kompetenz und personale Kompetenz für den Betroffenen markiert werden, mit bis zu sechs Einzelbegriffen (beispielsweise bei personaler Kompetenz die Fähigkeiten Flexibilität, Kreativität, Sorgfalt, Lernbereitschaft und Zuverlässigkeit). Weiter war es möglich, in Untermenüs zu den Aspekten der Motivation, Qualifikation und Leistungsfähigkeit Handlungsbedarfe zu formulieren. Im Bereich Sozialkompetenz wurden die Kategorien des Handlungsbedarfs weiter ausgeführt zu den Unteraspekten Erscheinungsbild, Sozialverhalten, Belastbarkeit. Bei weiteren Rahmenbedingungen ging es um die Unterbereiche Schulden und Langzeitarbeitslosigkeit.

Fraglich erschien insgesamt, woher die Erkenntnisse der Vermittlungsbeschäftigten zur Feststellung dieser differenzierten Kompetenzbewertungen kommen. Aufgrund des Verhältnisses von Mitarbeiterzahl und Kundenzahl lag nahe, dass es zeitlich schon schwer möglich ist, zu nur einem der ca. 20 Kompetenzfelder eine hinreichende Analyse durchzuführen, um belastbare Aussagen zu treffen. Zudem erschien fraglich, ob alle Vermittlungsbeschäftigte über eine hinreichend spezifische Ausbildung für die fachkundige Bewertung dieser komplexen Persönlichkeitsmerkmale verfügen. Jedenfalls war aus datenschutzrechtlicher Sicht zu vermeiden, dass derartige Bewertungen in charakterliche Feststellungen übergehen, mit der Gefahr, dass andere Bearbeiter diese Feststellungen fehlinterpretieren. Es sprach sehr viel dafür, dass die Bewertungsergebnisse nicht hinreichend valide sind.

Erhebungen zu den zuvor genannten Kriterien können zwar erforderlich sein, um mit entsprechenden Maßnahmen Vermittlungshindernisse abzubauen. Allerdings bedarf es dann einer gesicherten Tatsachengrundlage. Die gespeicherten Daten müssen aus datenschutzrechtlicher Sicht richtig sein. Falsche oder nicht ganz richtige Bewertungen sind nicht zulässig und dürfen nicht gespeichert werden. Im Falle der fehlenden Möglichkeit des Nachweises der Richtigkeit hat der Betroffene zu jedem vermerkten Datum einen Anspruch auf Löschung. Soweit die Unrichtigkeit nicht feststellbar ist, besteht ein Anspruch auf Dokumentation der ungeklärten Sachlage in geeigneter Weise (s. § 84 Abs. 1 SGB X).

Auch ist bedenklich, bei der Darstellung der Handlungsbedarfe zu den o. g. Kompetenzen eine Bewertung nach dem Schulnotensystem von Ziffer 1 bis Ziffer 6 zu vermerken. Hinweise zum Handlungsbedarf sind zwar notwendig, wenig aussagefähige Schulnotenbewertungen haben jedoch eher eine möglicherweise diskriminierende Wirkung.

Es wurde daher vom Landesbeauftragten empfohlen, Aspekte nur sachlich zu vermerken, wenn deren Vorliegen auf gesicherter Tatsachengrundlage festgestellt bzw. nachweisbar ist.

10.2.6 Jugendberufsagentur

Der Koalitionsvertrag für die 18. Legislaturperiode des Bundes sah die flächendeckende Einrichtung von Jugendberufsagenturen vor. Hilfen von Trägern der Grundsi-

cherung (SGB II), der Arbeitsförderung (SGB III) und der Jugendhilfe (SGB VIII) sollten gebündelt werden. Ziel war u. a. die rechtskreisübergreifende Zusammenarbeit zur Sicherung des Übergangs von der Schule in den Beruf, vor allem von besonders förderungsbedürftigen jungen Menschen. Vor Ort in den Landkreisen gab es hierzu bereits Initiativen. In Betracht gezogen wurde auch die Beteiligung von anderen Stellen, wie beispielsweise Schulen, Beratungsstellen und Weiterbildungseinrichtungen.

Aus datenschutzrechtlicher Sicht ist bei der Umsetzung von Hilfen zu berücksichtigen, dass die von den Sozialleistungsträgern erhobenen Daten als Sozialdaten einem besonderen Schutz unterliegen. Auch andere ggf. beteiligte Stellen bedürften für eine Zusammenarbeit unter Verwendung personenbezogener Daten hinreichender Rechtsgrundlagen. Soweit keine bereichsspezifischen Rechtgrundlagen (vgl. §§ 18a, 50 Abs. 1 SGB II) gegeben sind oder ausreichen, wäre eine informierte, freiwillige Einwilligung des jeweils Betroffenen notwendig.

Zur Unterstützung der Arbeit von Initiativen vor Ort hat das Bundesministerium für Arbeit und Soziales unter Beteiligung des Bundesministeriums für Familie, Senioren, Frauen und Jugend, der Bundesagentur für Arbeit, der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesländer und weiterer Einrichtungen eine Arbeitshilfe erstellt. Die dabei beteiligte Berliner Beauftragte für Datenschutz und Informationsfreiheit wurde vom Landesbeauftragten mit einigen Hinweisen zu notwendigen Änderungen der Entwürfe unterstützt. Die „Arbeitshilfe zum Sozialdatenschutz in Jugendberufsagenturen“ ist inzwischen im Internet öffentlich zugänglich. Die Frage nach einer entsprechenden Bundesdatei ist noch offen.

10.2.7 Zugriff auf Entwicklungsdokumentationen in Kindertagesstätten

Aus der Tagespresse konnte der Landesbeauftragte entnehmen, dass in einer Kindertagesstätte aus Dokumentationsordnern zu Kindern, u. a. mit Bildern und Entwicklungs- und Persönlichkeitsbeschreibungen, Unterlagen entwendet wurden. Nach Stellungnahme der die Einrichtung tragenden Stadt waren 11 Lerngeschichten von 11 verschiedenen Kindern betroffen. Die in den Gruppenräumen aufbewahrten Portfolios seien infolge der Vorgaben des Bildungsprogramms des Landes zwar für Eltern und Kinder zugänglich gewesen. Informationen zu Aktivitäten und Fotos von mehreren Kindern der Tagesstätte sind aber auch Unbefugten zur Kenntnis gelangt. Entwendete Fotos mit Vornamen verbunden mit Hinweisen auf Lieblingsspiel, -farbe, -essen usw. eröffneten die Möglichkeit der missbräuchlichen Verwendung der Daten.

Nach § 5 Abs. 3 Satz 2 KiFöG und dem auf der Homepage des Ministeriums für Arbeit, Soziales und Integration veröffentlichen Bildungsprogramm „Bildung: elementar – von Anfang an“ sind Kinder in Bezug auf Handeln, Mimik, Gestik, Sprache und Interaktion zu beobachten. Beobachtungen werden in Bezug auf Potentiale und Ressourcen sowie individuelle Lernstrategien – auch im Team – analysiert. Zu den Ressourcen gehören dabei erworbene wie genetisch angelegte sowie auch Umweltfaktoren, wie z. B. familiale Herkunft oder anregungsreiche Lebensumstände. Dies ist zu dokumentieren. Die Dokumentation ist nach dem Bildungsprogramm dem Kind und den Eltern „frei zugänglich“.

Dabei ist aber zu beachten, dass die in Kindertagesstätten erhobenen und gespeicherten Daten bei kommunal getragenen Einrichtungen Sozialdaten sind. Nach § 61 Abs. 1 Satz 3 SGB VIII gilt das SGB für die kommunalen Träger direkt. Im Übrigen ist

der Sozialdatenschutz für die freien Träger nach § 61 Abs. 3 SGB VIII durch entsprechende Vertragsgestaltung ebenfalls verbindlich vorzugeben. Sozialdaten (s. § 67 Abs. 1 Satz 1 SGB X) unterliegen dem Sozialgeheimnis nach § 35 Abs. 1 Satz 1 SGB I und bedürfen daher der über die allgemeine Schweigepflicht und Sorgfalt hinausgehenden besonderen Geheimhaltung. Der Schutz der Sozialdaten und damit auch der Schutz vor dem Zugriff anderer Personen als des betroffenen Kindes und seiner Eltern ist durch technische und organisatorische Maßnahmen sicherzustellen. Hinzu kommt noch, dass durch eine unbefugte Zugänglichmachung von Bildnissen der Kinder auch eine Verletzung des Rechts am eigenen Bild nach § 22 Abs. 1 KunstUrhG erfolgen kann.

Um einen Eindruck von der Situation in der Praxis zu erhalten, hat der Landesbeauftragte Kindertagesstätten aufgesucht. Dort wurde auf die vorgegebene Zugänglichkeit von Dokumentationen verwiesen. Es fanden sich in den Gruppenräumen in Griffhöhe für die Kinder bunte Ordner mit einem Foto des jeweiligen Kindes auf dem Rücken. In den Ordnern befanden sich viele Fotos, die das Kind in unterschiedlichen Aktionen und Situationen seines Kindertagesstättenalltags zeigen. Das jeweilige Kind war entweder allein oder im Vordergrund abgebildet, sodass es sich nicht um Bilder, sondern um geschützte Bildnisse im Sinne des Kunsturhebergesetzes handelte. Weitere, sensible Beobachtungen und Auswertungen befanden sich in nicht für Kinder zugänglichen Kinderakten mit weiteren Unterlagen zum Betreuungsverhältnis, die zum Teil verschlossen aufbewahrt wurden.

Das Ministerium für Arbeit, Soziales und Integration verwies zur Gewährleistung datenschutzrechtlicher Anforderungen auf „Vereinbarungen“ mit den Kindern und Erklärungen der Eltern im Betreuungsvertrag. Die „Vertragstreue“ von drei- bis fünfjährigen Kindern oder die im Kleingedruckten von Betreuungsverträgen einmal abgegebenen Erklärungen gewährleisten jedoch nicht allein ein dem Sozialdatenschutz und dem Schutz des Rechts am eigenen Bild angemessenes Sicherheitsniveau. Aus datenschutzrechtlicher Sicht bestehen zwar keine grundsätzlichen Bedenken, die Entwicklung des Kindes zu beobachten und zu dokumentieren, um den Entwicklungsprozess mit dem Kind und den Eltern gemeinsam zu gestalten. Der freie Zugriff eines Kindes und seiner Erziehungsberechtigten auf sein Portfolio kann daher selbstverständlich gewährt werden.

Andererseits gibt es Stoßzeiten, in denen die Kinder gebracht oder abgeholt werden, die einen unbeobachteten Zugriff Unbefugter bei freier Zugänglichkeit leicht möglich machen können. Dies gilt auch dann, wenn sich Eltern, die für das eigene Kind Zugang zu dem Bereich haben, in dem die Ordner stehen, andere Ordner nehmen. Die Möglichkeit des Zugriffs Unbefugter ist aber auszuschließen.

Der Zugriff und die Herausgabe bzw. Erörterung sensibler Informationen muss dem Personal vorbehalten bleiben. Die Unterlagen dürfen nicht offen zugänglich in offenen Regalen in den Gruppenräumen liegen. Sie sind in der Kinderakte in der Verwaltung, in abgeschlossenen Schränken oder abgeschlossenen Räumen aufzubewahren.

Bunte Ordner mit Fotos und lediglich deskriptiven Kommentaren für den Zugriff der Kinder, deren inhaltliches Niveau (wie bei den Überprüfungen festgestellt) nicht über ein Fotoalbum hinausgeht, können im Gruppenraum für Kinder zugänglich aufgestellt werden. Da eine Fotoverwendung über die unerlässlichen Vorgänge zur Gewährleis-

tung der Förderung in Tageseinrichtungen hinausgeht, greift für die Verwendung der Fotos keine gesetzliche Grundlage. Demgemäß war die Einwilligung einzuholen, die den Anforderungen des § 4 Abs. 2 DSG LSA bzw. § 4a BDSG entsprechen musste (informierte Einwilligung, Hinweis auf Verwendungszweck, hinreichend bestimmt, Schriftform, Hinweis auf Widerrufsrecht). Zudem sollten die Eltern auch ausdrücklich darin einwilligen, dass sich die Fotosammlungen der Kinder in der Tagesstätte im zugänglichen Bereich befinden dürfen.

Darüber hinaus sollte auch schon gegenüber den Kindern, wie zum Teil bereits praktiziert, klar vermittelt werden, dass ihnen der Zugriff nur auf den eigenen Ordner erlaubt ist. Für die Eltern bzw. anderen Begleiter der Kinder ist durch Vorabinformation und Aushang zu verdeutlichen, dass ein Zugriff auf die Ordner anderer Kinder zu unterbleiben hat. Zudem muss auch eine Aufsichtsperson zugegen sein, die die Einhaltung der Vorgaben sicherstellt. Ein unbeobachteter Zugang von Eltern oder anderen Personen, auch durch Reinigungskräfte, Hausmeister oder Handwerker, ist zu verhindern. Dies ist z. B. durch Abschließen der Räume zu gewährleisten, wenn keine Aufsichtsperson zugegen sein kann.

Auf diese Weise kann die fachlich gewünschte Arbeit mit und an den Portfolios möglich bleiben und zugleich den Gefahren für den Sozialdatenschutz und das Recht am eigenen Bild angemessen begegnet werden.

10.2.8 Pauschale Entbindung vom Bankgeheimnis

Ein Sozialamt legte einem Antragsteller für dessen Antrag auf Grundsicherung folgende Erklärung zur Unterschrift vor:

„Ich befreie das/die o. g. Institut/e vom Bankgeheimnis und den datenschutzrechtlichen Bestimmungen und beauftrage es, dem Sozialleistungsträger Auskünfte, insbesondere über den Kontostand und die Kontobewegungen, zu erteilen.“

Im Rahmen einer Beschwerde teilte der Antragsteller dem Landesbeauftragten mit, dass er Auskünfte über Kontostände und Kontobewegungen bereits erteile und durch Kontoauszüge belege. Ein begründeter Verdacht auf Sozialbetrug würde nicht vorliegen. Das Formular werde als stigmatisierend empfunden; Antragsteller würden dadurch in die kriminelle Ecke gedrängt und unter den Generalverdacht des Sozialbetrugs gestellt.

Zur Prüfung der Bedürftigkeit kann das Sozialamt grundsätzlich verlangen, dass es Kenntnis von dem Guthaben bzw. Vermögensverfügungen der letzten drei bis sechs Monate erhält. Rechtsgrundlage für die Forderung des Sozialamtes ist § 60 SGB I. Danach hat jeder, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des Leistungsträgers zu belegen.

Allerdings besteht keine Verpflichtung, eine entsprechende Befreiung vom Bankgeheimnis zu unterschreiben. Die Daten sind grundsätzlich beim Betroffenen zu erheben (§ 67a Abs. 2 SGB X). Das bedeutet, der Antragsteller hat im Rahmen seiner Mitwirkungspflicht die Unterlagen, z. B. die Kontoauszüge oder Sparbücher, selbst zu Verfügung zu stellen. So kann vermieden werden, dass das Geldinstitut von seinem Sozialleistungsbezug erfährt.

Das Sozialamt teilte mit, von der Ermächtigung noch nie Gebrauch gemacht zu haben, sodass eine Datenübermittlung an kontoführende Banken nicht erfolgt sei. Die Anfrage des Landesbeauftragten nahm das Sozialamt zum Anlass, auf die kritisierte Klausel zu verzichten.

10.2.9 Schweigepflichtentbindung im Versorgungsrecht

Sozialbehörden erheben vielfach medizinische Daten, um ihre Aufgaben erfüllen zu können. So ist es bei Versorgungsberechtigten nach dem Bundesversorgungsgesetz erforderlich, Daten darüber zu erheben, ob eine Arbeitsunfähigkeit schädigungsbedingt eingetreten ist. Denn dann besteht ggf. Anspruch auf höheres Versorgungskrankengeld gegenüber dem von Krankenkassen gezahlten Krankengeld. Die Sozialbehörden erheben die medizinischen Daten häufig auf der Grundlage einer schriftlichen Einwilligungs- bzw. Schweigepflichtentbindungserklärung.

Im Berichtszeitraum beschwerte sich eine niedergelassene Ärztin, dass die Sozialbehörde für die Prüfung eines Antrags auf Versorgungskrankengeld einen ausführlichen Befundbericht anforderte und dem Anliegen eine mehr als sechs Jahre alte Einverständniserklärung beilegte, die zweckgebunden für einen Verwaltungsvorgang des Jahres 2010 abgegeben worden ist. Die Patientin hatte der Ärztin nach Rücksprache mitgeteilt, dass diese Einverständniserklärung die Ärztin nicht mehr von ihrer ärztlichen Schweigepflicht entbinde. Die Ärztin bat die Sozialbehörde daraufhin um Vorlage einer aktuellen Einverständniserklärung. Statt eine aktuelle Einverständniserklärung zu übersenden, mahnte die Sozialbehörde die Ärztin und wies sie darauf hin, dass sie bei ausbleibender Rückantwort das zuständige Sozial- oder Amtsgericht um Vernehmung ersuchen werde und die Ärztekammer von dem Vernehmungsersuchen unterrichten werde.

Um Stellungnahme gebeten teilte die Sozialbehörde zunächst mit, dass keine rechtlich normierte Ablauffrist einer solchen Erklärung bestehe und die Erklärung nicht widerrufen worden sei. Der Landesbeauftragte erläuterte der Sozialbehörde, dass sich die Einverständniserklärung dem Wortlaut nach auf ein eingeleitetes Verwaltungsverfahren bezog, welches mit der Unanfechtbarkeit des Bescheides zu dem Verwaltungsverfahren erfahrungsgemäß endet.

Die Sozialbehörde entschloss sich daraufhin, die genutzten Vordrucke zu überprüfen und soweit erforderlich zu überarbeiten sowie das Verfahren hinsichtlich der Einhaltung der Zweckbindung der Schweigepflichtentbindungserklärung anzupassen. Eine nach datenschutzrechtlichen Vorgaben überarbeitete Einwilligungserklärung und Schweigepflichtentbindung unterzeichnete die Patientin nunmehr, sodass das Verfahren weitergeführt werden konnte.

Eine Einwilligungs- bzw. Schweigepflichtentbindungserklärung muss hinreichend bestimmt sein. Ausgeschlossen sind Pauschalermächtigungen, die für den Betroffenen nicht überschaubar Einwilligungen in mehrere Verfahren enthalten.

11 Beschäftigtendatenschutz

Auch in diesem Berichtszeitraum haben wieder viele Eingaben Anlass zur Prüfung und Beratung zum Umgang mit Beschäftigtendaten gegeben. Gegenstand von Anfragen war beispielsweise häufig die Verwendung von Daten aus der Telefonnutzung und dem E-Mail-Verkehr von Beschäftigten. Auch Fragen der Mitarbeiterüberwachung durch Video- oder GPS-Technik spielten eine Rolle (vgl. Nrn. 14.1.5 ff.). Allgemein wurde nach Möglichkeiten und Grenzen bei der Anwendung von Software gefragt. In den jeweiligen Aufgabenfeldern der Personalverwaltung ging es zumeist darum, welche Daten noch bzw. nicht mehr für die Verarbeitung erforderlich sind. In vielen Fällen wurde auch beklagt, dass unbefugte Zugriffe stattgefunden hätten.

Weiter wurden wieder einige kommunale Personalämter anlassunabhängig kontrolliert. Dabei konnten vielfältige Hinweise erteilt werden, u. a. zur Schriftgutentsorgung, zu Telearbeit, zu E-Mail und Internet am Arbeitsplatz und zur Aufbewahrung alter Bewerbungen.

11.1 Arbeitnehmerüberwachung

Der Landesbeauftragte macht auf zwei Gerichtsentscheidungen aufmerksam, in denen die hohen Anforderungen an die Verhältnismäßigkeit einer Überwachung von Beschäftigten verdeutlicht werden.

Das Recht auf Privatheit auch im Rahmen des Dienst- oder Arbeitsverhältnisses ist durch das Urteil des Europäischen Gerichtshofs für Menschenrechte vom 5. September 2017 (Application No. 61496/08, juris, ZD 2017, 571) gestärkt worden. Anlass der Entscheidung war eine Kündigung, die auf einer übermäßigen privaten Nutzung eines dienstlichen Instant Messaging Accounts beruhte, die durch unangekündigte Überwachung erkannt wurde. Die Arbeitgeber dürfen in engen Grenzen zwar Überwachungen durchführen, müssen dabei aber angemessene Maßnahmen gegen Missbrauch und Willkür ergreifen. Im Normalfall sollte vor einer Überwachung über Art und Inhalt informiert werden. Insbesondere der Zugriff auf Kommunikationsinhalte ist ein besonders schwerer Eingriff, der die Prüfung milderer Mittel erfordert. Schutzmaßnahmen müssen zudem sicherstellen, dass der Arbeitgeber solange nicht auf den Inhalt der Kommunikation zugreifen kann, wie der Arbeitnehmer nicht über die Zugriffsmöglichkeit informiert ist.

Das Bundesarbeitsgericht hatte mit Urteil vom 27. Juli 2017 (Az.: 2 AZR 681/16, juris, NJW 2017, 3258) entschieden, dass der Einsatz eines Software-Keyloggers, mit dem alle Tastatureingaben an einem dienstlichen Computer für eine verdeckte Überwachung und Kontrolle aufgezeichnet werden, nach § 32 Abs. 1 BDSG unzulässig war. Dies war der Fall, da kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung bestand. In dem zugrundeliegenden Fall war zwar pauschal von der Arbeitgeberin darauf hingewiesen worden, dass der gesamte „Internet-Traffic“ und die Benutzung ihrer Systeme „mitgeloggt“ werde. Es fehlte aber an einem auf Tatsachen beruhenden Verdacht einer Straftat oder schwerwiegenden Pflichtverletzung gegen den betreffenden Mitarbeiter. Die anlasslos veranlasste Überwachung war daher unverhältnismäßig.

11.2 Zeiterfassung mittels Fingerabdruck

In einer Eingabe wurde problematisiert, dass die Zeiterfassung in einem Versorgungszentrum mit vier Arztpraxen und insgesamt neun Beschäftigten mittels Fingerabdruck erfolgte. Auf Nachfrage erläuterte der Arbeitgeber, die Mitarbeiter hätten zuvor ihre Arbeitszeiten mit sog. Stundenzetteln erfasst. Nachweislich sei es mehrfach zum Arbeitszeitbetrug gekommen. Die Nutzung von sog. Stempeluhren scheide aus, da auch dabei Arbeitszeitbetrug stattfinden könnte. Die Mitarbeiter seien mit einer Arbeitsanweisung über das Fingerabdrucksystem informiert worden und hätten ihr schriftliches Einverständnis erklärt. Dagegen bestanden erhebliche datenschutzrechtliche Bedenken (zu einem entsprechenden Anliegen einer Kommune vgl. bereits XII. Tätigkeitsbericht, Nr. 12.3).

Eine Einwilligung der Beschäftigten lag zwar vor, war jedoch als Rechtsgrundlage nicht tragfähig. Wirksame Einwilligungen müssen stets freiwillig abgegeben werden. Davon ist im Beschäftigungsverhältnis infolge des Ungleichgewichts der Verhandlungsmacht in der Regel nicht auszugehen. Da den Beschäftigten keinerlei nachteilsfreie Alternativen angeboten wurden, lag hier eine die Freiwilligkeit ausschließende Drucksituation vor. Dies wurde auch in der übersandten Einwilligungserklärung deutlich, die als Arbeits-“Anweisung“ und Einverständniserklärung bezeichnet war.

Auch § 32 Abs. 1 Satz 1 BDSG (aktuell § 26 Abs. 1 BDSG 2018) bot in diesem Fall keine Rechtsgrundlage („zur Durchführung des Beschäftigungsverhältnisses …, verarbeiten …, wenn … erforderlich…“). Die Erfassung der Arbeitszeit von Beschäftigten ist legitimes Recht des Arbeitgebers. Beim Einsatz technischer Geräte ist im Rahmen der Erforderlichkeitsprüfung eine Abwägung der beteiligten Interessen erforderlich. Die legitimen Arbeitgeberinteressen sind mit dem gebotenen Schutz der Persönlichkeitsrechte der Betroffenen abzuwägen.

Die Verwendung eines Zeiterfassungssystems, das Fingerabdrücke und damit besonders sensible Daten nutzt, war jedoch nicht erforderlich und erst recht nicht verhältnismäßig im engeren Sinne. Das Ziel der Erfassung der Arbeitszeit konnte keinen so weitreichenden Eingriff rechtfertigen. Fingerabdrucksysteme greifen in erheblichem Maß in das Persönlichkeitsrecht der Betroffenen ein. Das eindeutige lebenslange Erkennungsmerkmal ist digital dauerhaft personenbezogen beim Arbeitgeber gespeichert. Es unterliegt damit seinem permanenten Zugriff, und ggf. weiterer Beschäftigter und Wartungs-Vertragspartner. Dies eröffnet Verlust- und Missbrauchsgefahren.

Biometrie im Beschäftigungsverhältnis ist zwar nicht grundsätzlich ausgeschlossen. So können auch erhebliche Eingriffe in das Persönlichkeitsrecht der Beschäftigten gerechtfertigt sein, wenn ein besonders hoher Schutzbedarf besteht. Dies kann beispielsweise beim Zugang zu Hochsicherheitszonen in Atomkraftwerken oder Rüstungsbetrieben der Fall sein. Dabei geht es aber vorrangig nur darum, den Zugang zu eröffnen. Dies erfordert nicht, die Fingerabdruckdaten personenbezogen weiter zu verarbeiten. Ausreichend ist eine Verifikation, ein 1:1-Abgleich des konkreten Fingers mit einem nicht rückführbaren biometrischen Referenzmerkmal (Template bzw. biometrische Signatur), ohne dass der Zusammenhang zwischen Referenzmerkmal und Person ohne Weiteres recherchierbar wird.

Im Rahmen der Abwägung im konkreten Fall der Zeiterfassung war zwar auch zu berücksichtigen, dass es um kündigungsrechtlich und strafrechtlich relevantes Verhalten des Arbeitszeitbetruges ging, jedoch die absolute Höhe geringe finanzielle Beträge betraf (Arbeitszeitbetrug im großen Stil wäre auch ohne Erfassung aufgefallen). Fast alle Zeiterfassungssysteme kommen ohne Fingerabdrücke aus. Zudem ist zu berücksichtigen, dass die Sicherheit von Fingerabdrucksystemen relativ gering ist, da ein Fingerabdruck wohl leicht nachzumachen ist. Die in mobilen Geräten verbauten Fingerabdrucksensoren bieten daher eher Komfortgewinn gegenüber der Passwort- oder Mustereingabe, aber nur bedingt Verbesserung der Sicherheit.

Dem Versorgungszentrum wurde daher aufgegeben, zur Erforderlichkeit des Fingerabdrucksystems eine Konkretisierung zum behaupteten Arbeitszeitbetrug vorzunehmen (Schadensumfang, polizeiliche Anzeige, Art und Weise und Zeitraum des Arbeitszeitbetruges, eingesetzte oder zumindest geprüfte Alternativmaßnahmen). Nicht nachvollziehbar war auch, aus welchem Grund persönliche Kontrollen zu verschiedenen Uhrzeiten in zwei kleinen Einheiten mit insgesamt neun Mitarbeitern nicht möglich sein sollen (z. B. in Zeiträumen des Arbeitszeitbeginns und Arbeitszeitendes). Weiter wurde auf die strengen Vorgaben von § 32 Abs. 1 Satz 2 BDSG (aktuell § 26 Abs. 1 Satz 2 BDSG 2018) hingewiesen.

Zudem waren technische und sicherheitsrelevante Fragen zu berücksichtigen, wie die Methode zur Bildung eines Referenzmerkmals zum jeweiligen Fingerabdruck. Zu klären war, ob Rohdaten gespeichert werden würden oder mathematische Werte, die eine Rekonstruktion der Ursprungsdaten ausschließen. Auch wären Erläuterungen geboten gewesen, ob die Einstellungen zu den Rückweisungsquoten (Fingerabdruck wird nicht erkannt oder akzeptiert) mit den Beschäftigteninteressen vereinbar sind (Gefahr unangemessenen Rechtfertigungsdrucks). Zudem wären Maßnahmen des Zugriffschutzes vorzunehmen gewesen.

Nachdem die Komplexität der Thematik und die Fülle der Anforderungen durch die aufgeworfenen Fragen ersichtlich wurden, hat das Versorgungzentrum mitgeteilt, auf die Nutzung des Fingerabdrucksystems zu verzichten.

12 Finanzen, Kataster, Kommunales und Statistik

12.1 Entwicklung der Kontendatenabrufe

Auch im zurückliegenden Berichtszeitraum nahm die Anzahl der durchgeführten Kontendatenabrufe weiterhin zu (vgl. XII. Tätigkeitsbericht, Nr. 13.1). Im Jahr 2017 wurden im Durchschnitt monatlich 1700 Kontendaten durch öffentliche Stellen des Landes beim Bundeszentralamt für Steuern abgefragt.

Bei einem Kontendatenabruf werden den zum Abruf berechtigten Stellen zu einer Person die bestehenden Konten mitgeteilt, über die diese Person verfügt. Über diese Daten gibt es nach § 24c Kreditwesengesetz eine Datei. In dieser Datei wird nicht gespeichert, ob sich auf einem Konto ein Guthaben befindet. Somit erfolgt auch keine Mitteilung zur Höhe eines eventuellen Guthabens an die abrufende Stelle.

Besonders auffällig ist die stark wachsende Zahl der Kontendatenabrufe durch Gerichtsvollzieher. Diese dürfen seit 2013 Kontendaten über das Bundeszentralamt für

Steuern abrufen (§ 93 Abs. 8 Satz 2 AO), wenn der Schuldner seiner Pflicht zur Abgabe einer Vermögensauskunft nicht nachkommt bzw. das Vermögen des Schuldners nicht zur Begleichung seiner Schulden ausreicht. Der Gerichtsvollzieher hat darüber hinaus auch noch das Recht, bei den Trägern der gesetzlichen Rentenversicherung, beim derzeitigen Arbeitgeber oder beim Kraftfahrt-Bundesamt die Kontendaten und bei letzterem auch die Fahrzeug- bzw. Halterdaten eines Fahrzeuges abzufragen.

Seit Änderung der ZPO von Ende 2016 darf der Gerichtsvollzieher auch Kontendaten abfragen, wenn die einzutreibenden Schulden den Betrag von 500,00 € unterschreiten. Dies hat zur Folge, dass sich die jährlichen Zahlen der Abrufe der Kontendaten zu Vollstreckungszwecken durch Gerichtsvollzieher im Zeitraum des Tätigkeitsberichts mehr als verdoppelten.

In der Praxis hat sich ein Wandel dahingehend vollzogen, dass in vielen Fällen von einer Sachpfändung in das bewegliche Vermögen eines Schuldners abgesehen wird, da z. B. viele technische Geräte einem schnellen Wertverlust unterliegen. Stattdessen wird von den Gläubigern eine Beitreibung von Geldforderungen bei den Gerichtsvollziehern beauftragt.

Vor diesem Hintergrund hat sich der Landesbeauftragte das Verfahren, welches durch Gerichtsvollzieher für die Durchführung der Zwangsvollstreckung wegen Geldforderungen durchzuführen ist, erläutern lassen. Dabei konnte festgestellt werden, dass durch Software mit Musterschreiben und Dokumentationsblättern den Gerichtsvollziehern Mittel zur Verfügung stehen, durch die der Gerichtsvollzieher seinen gesetzlich vorgeschriebenen Hinweis- und Dokumentationspflichten nachkommen kann. Diese Blätter werden dann zur Akte des jeweiligen Schuldners genommen.

Die Gerichtsvollzieher haben insofern gesetzlich vorgeschriebene Formalien zu beachten. So ist der Schuldner über das Kontendatenabrufverfahren zu informieren. Daten, die der Gerichtsvollzieher erhält, die aber für die Vollstreckung nicht erforderlich sind, sind zu löschen. Das ganze Abrufverfahren muss protokolliert werden.

12.2 Verarbeitung von Steuerdaten – Staatsvertrag zur länderübergreifenden Verfahrensbetreuung

Der Landesbeauftragte wurde durch das Ministerium der Finanzen im Herbst 2016 davon in Kenntnis gesetzt, dass im Bereich der Steuerverwaltung eine engere Zusammenarbeit unter den Ländern Bremen, Mecklenburg-Vorpommern, Niedersachsen, Schleswig-Holstein und Sachsen-Anhalt geplant sei.

Aufgrund von bereits bestehenden Vereinbarungen aus dem Vorhaben KONSENS (s. IX. Tätigkeitsbericht, Nr. 9.6) werden in allen Bundesländern für steuerrechtliche Verfahren von Steuern, die durch Bundesrecht geregelt sind, einheitliche Programme entwickelt und genutzt. Durch eine zusätzliche, länderübergreifende Verfahrensbetreuung versprechen sich die o. a. Länder umfangreiche Synergieeffekte. So sollte für jedes Programm ein Land als zentraler Verfahrensbetreuer benannt werden.

Der zentrale Verfahrensbetreuer ist für das jeweilige Fachverfahren zuständig und übernimmt damit die Aufgaben der Erstellung der erforderlichen Verfahrensdokumentationen. Dabei werden auch die Auswirkungen des neuen Verfahrens auf die

bisherigen Verfahren und Abläufe bewertet und Schulungsbedarfe ermittelt. Gleichzeitig ist der zentrale Verfahrensbetreuer im Betrieb des jeweiligen Verfahrens für die Analyse und Behebung von Störungen zuständig. Der Staatsvertrag soll als rechtliche Grundlage für den Abschluss von Vereinbarungen dienen, in welchen detailliert geregelt wird, für welches Verfahren welches Land die zentrale Verfahrensbetreuung übernimmt. In diesen Vereinbarungen wird auch der konkrete Umfang der Aufgaben bestimmt, welche durch das Land, das zentraler Verfahrensbetreuer ist, für jedes einzelne andere Land übernommen werden.

Der Landesbeauftragte, aber auch die Landesbeauftragten der anderen beteiligten Länder, gaben Hinweise zu Formulierungen des Staatsvertrages ab. Vor allem wurde darauf verwiesen, dass Formulierungen bereits zum damaligen Zeitpunkt sinnvollerweise an die Definitionen der DS-GVO angepasst werden sollten, um nicht nach dem 25. Mai 2018 den Staatsvertrag erneut anfassen zu müssen.

Im Verlauf der Vertragsverhandlungen kamen Änderungen von Gesetzen hinzu, die u. a. eine Grundlage für die Verarbeitung von personenbezogenen Daten im Steuerverfahren bilden. So wurde die Abgabenordnung geändert und z. B. die Datenschutzaufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der AO auf die Bundesbeauftragte für Datenschutz und Informationsfreiheit ab dem 25. Mai 2018 übertragen (siehe Nr. 12.3) und ein KONSENS-Gesetz (s. Nr. 12.4) verabschiedet, durch welches die Länder verpflichtet werden, einheitliche IT-Verfahren sowie Software für die Verbesserung oder Erleichterung des gleichmäßigen Vollzugs der von den Ländern im Auftrag des Bundes verwalteten Steuern einzusetzen.

Der Entwurf des Staatsvertrages wurde an diese gesetzlichen Änderungen jedoch nicht mehr angepasst. Er wurde im August/September 2017 unterschrieben und im November 2017 dem Landtag zur Ratifizierung vorgelegt. Mit Gesetz zum Staatsvertrag vom 16. Januar 2018 (GVBl. LSA S. 2) wurde der Staatsvertrag veröffentlicht; er trat am 1. Juni 2018 in Kraft.

12.3 Auskunftsrecht nach Abgabenordnung

In seinem XI. Tätigkeitsbericht (Nr. 12.1) hat der Landesbeauftragte über einen Entwurf zu gesetzlichen Regelungen zum Auskunftsrecht für Betroffene im Steuerverfahren berichtet. Dieser wurde aber nicht weiterverfolgt.

Ende Mai 2017 erhielten die Landesdatenschutzbeauftragten Kenntnis von einem Änderungsantrag zu einem Artikelgesetz (BT, Ausschuss für Arbeit und Soziales, Ausschussdrucksache 18(11)1031 vom 16. Mai 2017), mit welchem nicht nur das Auskunftsrecht in der AO, sondern auch die datenschutzrechtliche Aufsicht im Anwendungsbereich der AO über die Landesfinanzbehörden und die Kommunalfinanzbehörden, soweit sie für die Erhebung der Realsteuern zuständig sind (zuständige Aufsichtsbehörde wird die Bundesbeauftragte), geändert werden sollte. Das eilige Vorgehen wurde mit der Anpassung der AO an die Vorschriften der Datenschutz-Grundverordnung (DS-GVO) begründet.

Den Landesbeauftragten für den Datenschutz blieb keine Zeit, die geplanten rechtlichen Änderungen datenschutzrechtlich zu bewerten und eine detaillierte Stellungnahme abzugeben, zumal mit diesem Änderungsantrag auch eine ganze Reihe wei-

terer Gesetzesänderungen in den bereits vorliegenden Entwurf eines Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften (BT-Drs. 18/12041) eingebracht wurden. Am 17. Juli 2017 wurde das Gesetz beschlossen (BGBl. I S. 2541). Der Art. 17 des Gesetzes beinhaltet die o. a. Änderungen der AO.

Die neuen Regelungen zum Auskunftsrecht im Steuerverfahren in der AO schränken die „Rechte der betroffenen Person“ im III. Kapitel der DS-GVO ein. Somit gelten die Pflichten, die sich insbesondere aus den Art. 13 bis 15 der DS-GVO ergeben, für Finanzbehörden nur eingeschränkt.

12.4 KONSENS-Gesetz

Im Zusammenhang mit der Neuregelung des bundesstaatlichen Finanzausgleichsystems ab dem Jahr 2020 hat der Bundestag ein Artikelgesetz verabschiedet, mit welchem eine große Anzahl von Bundesgesetzen geändert wurden, die Auswirkungen auf finanzielle Verpflichtungen und Entwicklungen der Länder haben. Dabei wurde auch ein Gesetz über die Koordinierung der Entwicklung und des Einsatzes neuer Software der Steuerverwaltung (KONSENS-Gesetz, BGBl. I 2017, S. 3122, 3129) verabschiedet.

Bereits im IX. Tätigkeitsbericht (Nr. 9.6) hat der Landesbeauftragte zum Projekt KONSENS berichtet. Durch die Vereinheitlichung der Steuersoftware sollten die Länder in die Lage versetzt werden, schneller und vor allem einheitlich Steuern zu berechnen.

Durch das KONSENS-Gesetz wurden nunmehr Einzelheiten festgelegt, die die Entwicklung von IT-Verfahren und Software, sowie deren Einsatz, Pflege und Wartung für alle Länder ab Januar 2019 regeln und den einheitlichen Einsatz dieser IT-Verfahren und der entwickelten Software vorschreiben. Dies betrifft die Veranlagung und Berechnung aller Steuern, die durch die Länder im Auftrag des Bundes verwaltet werden. Damit hat sich die bisherige Verwaltungsvereinbarung zur gemeinsamen Entwicklung und Nutzung der Steuersoftware erledigt.

12.5 Energieatlas

Der Landesbeauftragte wurde von einer Hochschule um Beratung gebeten, die im Zusammenwirken mit einer Stadt ein Programm entwickelt hat, das die Darstellung von Solarenergieeignung und Geothermieeignung von Gebäuden und Grundflächen nebst Berechnungsmöglichkeiten für Internetnutzer enthalten sollte.

Informationen zur Solarenergieeignung oder Geothermieeignung in Bezug auf einzelne Grundstücke oder Gebäude sind personenbeziehbare Daten und unterliegen daher datenschutzrechtlichen Restriktionen. Sie treffen wertbildende Aussagen zu den Grundstücken bzw. Gebäuden und beschreiben damit Einzelpersonen betreffende Sachverhalte. Luftbilder, kartographische Darstellungen, Georeferenzierungen, Angaben von Straße, Lage und ggf. Hausnummer ermöglichen die Zuordnung der Informationen zu den jeweiligen Eigentümern. Diese sind auf verschiedene Weise (u. a. Grundbuchamtsauskunft) ohne unverhältnismäßigen Aufwand zu ermitteln.

Eine interne Verwendung von zusammengestellten Daten zur Erfüllung kommunaler Aufgaben könnte auf der Grundlage von § 10 Abs. 1 DSG LSA möglich sein. Ein Beispiel ist die eigene Auswertung zur Erstellung integrierter energetischer Quartierkonzepte für KfW-Förderprogramme.

Grundlage einer Datenübermittlung könnte § 12 DSG LSA sein. Die Ausschöpfung aller Möglichkeiten von Programmen, die Solarenergie- bzw. Geothermiekataster ermöglichen, ist jedoch problematisch. Der Informationsgehalt zum jeweiligen Grundstück bzw. Gebäude kann sehr differenziert sein (u. a. Prognosen zu nutzbaren qm, konkrete Daten zur Globalstrahlung, kWh/a-Angaben). Nutzungsmöglichkeiten der Grundstücke und wertbildende Faktoren könnten bereits berechnet/berechenbar dargestellt sein (Ertragsrechner, Kosten etc.). Bei Datenübermittlungen an die Bevölkerung, zumal über das Internet, läge dann ein nicht durch die städtischen Aufgaben gerechtfertigter Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung vor. Geothermie- und klimabezogene Vorhaben einer Kommune sind zwar anzuerkennen. Diesen Anliegen kann aber mit datenschutzfreundlicheren Mitteln Rechnung getragen werden (allgemeine Hinweise zum Solarenergieprogramm mittels Informationsbroschüren, Tageszeitung, Postsendungen, Rundfunk etc.).

Zulässigkeit und Rechtsgrundlagen der Veröffentlichung sog. Energieatlanten oder Solarkataster im Internet sind noch nicht verbindlich geklärt. In der Praxis wird zumeist davon ausgegangen, dass es sich bei den in Energieatlanten oder Solarkatastern gespeicherten Daten um Umweltinformationen handelt, die nach Maßgabe der Umweltinformationsgesetze des Bundes und der Länder veröffentlicht werden dürfen. Dies setzt insbesondere voraus, dass einer Veröffentlichung keine Ausschlussgründe, wie z. B. der Schutz personenbezogener Daten, von Betriebs- und Geschäftsgeheimnissen oder des Statistikgeheimnisses, entgegenstehen. Soweit durch die Veröffentlichung personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt werden, kommt nach § 10 Abs. 6 UIG i. V. m. § 9 Abs. 1 Nr. 1 UIG eine Veröffentlichung grundsätzlich nicht in Betracht, es sei denn die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. Die betroffenen Personen sind nach § 9 Abs. 1 Satz 3 UIG zudem vor der Entscheidung über die Veröffentlichung zwingend anzuhören.

Die in derartigen Projekten bezeichneten Daten könnten auch unter die „Geodaten“ im Sinne des § 3 Abs. 1 Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt (GDIG LSA) fallen – insbesondere Sonnen- und Windenergie werden nach Anhang III Nr. 20 der INSPIRE-Richtlinie (Amtsblatt der Europäischen Union L 108/1) dem Begriff „Geodaten“ zugeordnet. Die Veröffentlichung von Geodaten ist in § 9 i. V. m. §§ 10 und 11 GDIG LSA geregelt. Auch hier ist eine Anhörung geboten (§ 10 Abs. 2 Satz 3 GDIG LSA). Die Prüfung der Veröffentlichung von Geodaten nach dem GDIG LSA erfolgt im Grundsatz nach den zuvor für das Umweltinformationsrecht geschilderten Kriterien. Bei einer Offenbarung personenbezogener Daten führt jedoch bereits jede Beeinträchtigung eines schutzwürdigen Interesses zum Ausschluss des Informationszugangs, sofern nicht ausnahmsweise das öffentliche Interesse am Zugang überwiegt. Allerdings gelten die Vorgaben des Gesetzes nach § 4 Abs. 4 GDIG LSA im kommunalen Bereich nur, wenn die Erfassung und Bereitstellung der Daten gesetzlich vorgeschrieben ist. Dies wäre jeweils zu prüfen.

Im Ergebnis könnte die Veröffentlichung von auf einzelne Grundstücke beziehbaren Daten zur Solarenergieeignung bzw. zur Geothermie in gewissem Umfang möglich sein.

Die Anhörung ist grundsätzlich im Einzelfall durchzuführen, da Zweck der Anhörung die Klärung der Frage ist, ob der Betroffene der Preisgabe seiner Daten zustimmt oder ob das öffentliche Interesse an der Offenbarung gegenüber den Interessen des jeweils Betroffenen überwiegt. Eine besondere Form der Anhörung ist in den genannten Vorschriften nicht vorgegeben. Entsprechend § 10 Verwaltungsverfahrensgesetz (die Regelungen des § 10 VwVfG gelten sinngemäß auch für andere Bereiche des Verwaltungshandelns) ist auch für die Anhörung von der Nichtförmlichkeit auszugehen. Eine Anhörung wäre daher einfach, zweckmäßig, zügig und unter Beachtung des Verhältnismäßigkeitsgrundsatzes durchzuführen. Ob dies aus Gründen der Praktikabilität über eine Information durch Veröffentlichung in Tageszeitungen und/oder im Amtsblatt hinreichend möglich ist, könnte fraglich sein. Denkbar wäre eine Versendung einer umfassenden Information mit dem Grundsteuerbescheid, verbunden mit der Aufforderung, eventuelle Bedenken mitzuteilen. So könnte es gelingen, die Betroffenen zu erreichen.

Weiter erfordert die Veröffentlichung eine Abwägung der öffentlichen Interessen an der Bekanntgabe mit den schutzwürdigen Interessen der Grundeigentümer.

Fraglich ist hierbei, worin das besondere öffentliche Interesse daran besteht, dass jedermann sich nicht nur über die Energiepotentiale seines eigenen Grundstücks, sondern auch über die jedes anderen Grundstücks informieren können soll. Wird beispielsweise eine positive Energiesparprognose zu einem bestimmten Grundstück veröffentlicht, wird der Eigentümer ggf. langfristig mit spezifischer Werbung belästigt. Zudem könnte er gegenüber kritischen Nachbarn oder Freunden in „Rechtfertigungszwang“ gebracht werden, wenn er die Potentiale zum Schaden der Umwelt nicht nutzt. Weiter sind die Informationen wertbildend, was bei einer Veräußerung bei „Nichteignung“ zu erheblicher Reduzierung des Kaufpreises führen kann. Vor diesem Hintergrund wäre zumindest ein Ausschöpfen umfassender Informationsmöglichkeiten gegenüber der breiten Öffentlichkeit bedenklich.

Die Veröffentlichung entsprechender Energiekataster betrifft aber Fragen des Klimaschutzes. Die staatliche Verantwortung für den Schutz natürlicher Lebensgrundlagen hat Verfassungsrang (Art. 20a GG, Art. 35 Abs. 1 Verf LSA) und ist als öffentliches Interesse zu berücksichtigen. Dies gilt auch für eine kommunale Verwaltung und deren Handeln bei der Stadtentwicklung. Gleichzeitig werden auch Informationsbedürfnisse von einzelnen Grundstückseigentümern und Anbietern von entsprechenden Anlagen erfüllt.

Eine zulässige Veröffentlichung von Energiekatastern kommt daher nur dann in Betracht, wenn es gelingt, die durch die dargestellten Informationen (Werte, Berechnungen) möglichen Beeinträchtigungen der Betroffenen zu reduzieren. Zu denken wäre an eine begrenzte Information zu Energiepotentialen im Internet, bei der der Informationsgehalt nur wenig über das hinausgeht, was anderweitig einfach in Erfahrung gebracht werden kann (z. B. durch Google Earth, Objektbesichtigung, Nachbarbefragung). Vor diesem Hintergrund könnte ein Solarkataster vertretbar erscheinen, dass die Öffentlichkeit via Internet nur darüber informiert, ob ein Gebäude für die Anbringung von Solarenergieanlagen „gut geeignet“, „(noch) geeignet“ oder „weniger

geeignet“ ist. Interessierte Grundstückseigentümer hätten dann die Möglichkeit, durch Anfragen bei der Stadtverwaltung Detailinformationen zu ihrem eigenen Grundstück zu erhalten.

Ein ähnliches Vorgehen dürfte sich auch für den weiteren Bereich der Geothermie empfehlen. Die vollflächige Darstellung zur Geothermieeignung einzelner Stadtviertel lässt zumindest dann, wenn das gesamte Gebiet mit der gleichen Farbdarstellung gekennzeichnet ist, den Schluss zu, dass die damit verbundene Aussage auf alle dort gelegenen Grundstücke zutrifft. Zur Vermeidung einer übermäßigen individuellen Betroffenheit ist es geboten, die mit der Farbdarstellung verbundenen Von-Bis-Angaben zu energierelevanten Merkmalen auf hinreichend pauschal gekennzeichnete Bereiche zu beziehen.

12.6 Veröffentlichung personenbezogener Daten im Ratsinformationssystem

Immer wieder geben Veröffentlichungen von Sitzungsunterlagen und Beschlüssen der Kommunen Anlass zur Beschwerde beim Landesbeauftragten.

Grundsätzlich schreiben Regelungen im Kommunalverfassungsgesetz (§ 52 KVG) vor, wann eine Sitzung der Vertretung und ihrer Ausschüsse öffentlich stattfinden soll. Für die Vorbereitung eines solchen Sitzungsteils werden von den Kommunen oft auch bereits die Hintergrund-Dokumente im für jedermann zugänglichen Teil des Ratsinformationssystems mitveröffentlicht. Manche dieser den Tagungsordnungspunkt vorbereitenden Dokumente beinhalten personenbezogene oder personenbeziehbare Daten. Eine Rechtsgrundlage für die Veröffentlichung dieser personenbezogenen Daten ist in den meisten Fällen nicht gegeben. Selbst wenn der Themenkomplex im öffentlichen Teil einer Sitzung zu behandeln ist, handelt es sich bei der Internetveröffentlichung um einen anderen Kreis der Öffentlichkeit, welche Kenntnis von den personenbezogenen oder personenbeziehbaren Daten erhält. Es geht dabei letztlich um eine Übermittlung personenbezogener Daten in alle Welt. Ein angemessenes Datenschutzniveau, welches mit dem in Deutschland vergleichbar, oder zukünftig mit dem Datenschutzniveau Europas ist, kann aber nicht weltweit gewährleistet werden. Somit wäre eine Datenübermittlung ins Ausland nur unter den Voraussetzungen des § 13 Abs. 2 Satz 3 DSG LSA zulässig. Folglich müsste in den meisten Fällen also die Einwilligung der Betroffenen in die Übermittlung der Daten vorliegen, was jedoch häufig nicht der Fall ist.

Mit der Regelung zur Medienöffentlichkeit im KVG wurde zwar die Übertragung von öffentlichen Sitzungen im Internet zugelassen (vgl. XII. Tätigkeitsbericht, Nr. 13.4.1), daraus ergibt sich aber keine Berechtigung zur Veröffentlichung jeglicher Sitzungsunterlagen.

Bei Veröffentlichungen der Unterlagen von Sitzungen der Vertretungen der Kommune im öffentlichen Teil des Ratsinformationssystems muss von der verantwortlichen Stelle gewissenhaft geprüft werden, ob eine Veröffentlichung personenbezogener Daten zulässig ist.

12.7 Asylbewerbermanagementsystem Sachsen-Anhalt (ABES)

Nachdem auch das Land Sachsen-Anhalt vermehrt Flüchtlinge zugewiesen bekommen hat, die durch die zuständigen Behörden registriert, durch Ärzte untersucht und auf Landkreise und Gemeinden verteilt werden mussten, wurde überlegt, wie das Verfahren der Datenerhebungen, der notwendigen Datenübermittlungen sowie die Nutzung der Daten der Flüchtlinge durch die zuständigen Stellen in einem sicheren IT-Fachverfahren geregelt werden kann.

Der Landesbeauftragte wurde durch das zuständige Ministerium für Inneres und Sport (MI) in die Planung zur Einführung des Asylbewerbermanagementsystems Sachsen-Anhalt „ABES“ (früherer Begriff: Asylbewerbererfassungssystem) von Anfang an einbezogen. Das Asylbewerbermanagementsystem wird von einer privaten IT-Firma in Zusammenarbeit mit dem MI und den das Fachverfahren nutzenden Behörden (vertreten im Nutzerbeirat) bedarfsorientiert entwickelt und kontinuierlich verbessert. Im Nutzerbeirat sind die wichtigsten Beteiligten – wie etwa die Zentrale Anlaufstelle Sachsen-Anhalt in Halberstadt, Landeserstaufnahmeeinrichtungen in Magdeburg, Klietz, zukünftig auch in Bernburg, der Landkreis Harz, das Landesverwaltungsamt, das MI nicht nur als Auftraggeber und auch der Auftragnehmer, sowie auch der Landesbeauftragte – vertreten, sodass Fehler schnell behoben und Forderungen nach neuen Funktionen zentral aufgenommen, diskutiert, priorisiert und zügig beauftragt und umgesetzt werden können. Aufgrund der fortlaufenden Entwicklung des Programms, wobei auch ständig Neuerungen durch gesetzliche Änderungen eingearbeitet werden, finden datenschutzrechtliche Belange frühzeitig Berücksichtigung.

Aufgabe von ABES ist die zentrale Bereitstellung von Diensten für die Abwicklung von Erstaufnahme, Rückkehrmanagement und Unterbringung durch die im Nutzerbeirat vertretenen Stellen und zugehörigen Behörden wie Gesundheitsämter, Sozialämter, Ausländerbehörden und Jugendämter. Auch Zugriffe Dritter, wie des Wachdienstes, der Küche oder von Hilfsdiensten wie den Johannitern oder dem DRK sind möglich. Andere – z. B. die Polizei – haben Interesse bekundet, Zugriff auf ABES zu bekommen. Alle benötigen spezifische Zugriffsrechte. Im ABES sind die personenbezogenen Daten der Betroffenen hinterlegt, die für das Ausfüllen von Formularen bei den vorgenannten Ämtern, den Druck von Heimausweisen und die allgemeine Verwaltung (Sprache, Familienstrukturen, Religion, Abwesenheiten, …) benötigt werden. Diese werden mit dem Ausländerzentralregister synchronisiert bzw. passend aktualisiert. Für alle Funktionen werden im Nutzerbeirat Konzepte erarbeitet, die auch den Datenkatalog beinhalten, der erhoben werden muss, Rollen festgelegt, welche Stelle wann auf welche Daten zugreifen darf, und Musterschreiben hinterlegt, die für die verschiedenen Bearbeitungsvorgänge im Asylverfahren genutzt werden können.

Eine abschließende datenschutzrechtliche Bewertung der Zugriffe auf die Daten der Asylbewerber durch die einzelnen Rollen steht noch aus.

12.8 Bewachungsunternehmen in Unterkünften für Ausländerinnen und Ausländer

Nach einer Angabe des Bundesamtes für Migration und Flüchtlinge stellten in Sachsen-Anhalt allein im Jahre 2015 über 17.000 Personen einen Asylantrag. Asylsuchende werden auch in Gemeinschaftsunterkünften untergebracht. Die Aufnahme und letztendlich die Unterbringung obliegen dabei gem. § 1 Abs. 1 AufnG den Landkreisen und kreisfreien Städten. Um die Asylsuchenden vor internen und externen Gefahrenlagen zu schützen, werden in verschiedenen Unterkünften in Sachsen-Anhalt im Auftrag der aufnehmenden Kommunen bzw. Landkreise oder im Auftrag der Unterkunftsbetreiber Unternehmen des Bewachungsgewerbes gem. § 34a GewO eingesetzt.

Das Ministerium für Inneres und Sport (MI) machte den Landesbeauftragten darauf aufmerksam, dass außer in § 34a GewO i. V. m. der Bewachungsverordnung für Bewachungsunternehmen kaum Vorgaben zur Zuverlässigkeitsüberprüfung der Betreiber und der Wachpersonen existieren. Dies nahm das MI zum Anlass, dem Landesbeauftragten den Entwurf eines Erlasses zur datenschutzrechtlichen Stellungnahme vorzulegen, der einen Rahmen für die Anforderungen an die Qualitätskriterien von Bewachungsdienstleistungen, zur Qualifikation des Sicherheitspersonals, zum Einsatz von Bewachungsunternehmen als Subunternehmen und vor allem für die Unbedenklichkeitsprüfung des Bewachungspersonals festlegt. Im Besonderen bei der Unbedenklichkeitsprüfung hatte der Erlassentwurf zwischen den Grundrechten der eingesetzten Wachpersonen einerseits und der Sicherstellung eines ordnungsgemäßen Einsatzes geeigneter Wachpersonen andererseits abzuwägen.

Kern der Kritik des Landesbeauftragten war die vorgesehene Einverständniserklärung der Wachpersonen in die Prüfung ihrer Unbedenklichkeit. Dieser Erklärung fehlte eine wichtige Voraussetzung, nämlich die Freiwilligkeit, von der wegen des Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer nicht in jedem Fall auszugehen ist. Auf Basis der Einverständniserklärung kommt es zu einer Fülle von Übermittlungen sensibler personenbezogener Daten der Betroffenen zwischen dem Bewachungsunternehmen oder ggf. dem Betreiber der Unterkunft, der Aufnahmekommune, der Polizei und der Verfassungsschutzbehörde. Letztendlich führt dies dazu, dass ein Bewachungsunternehmen erfährt, dass ein oder mehrere seiner Arbeitnehmer zwar nach wie vor die nach § 34a GewO genannten Voraussetzungen für die Durchführung von allgemeinen Bewachungsaufgaben erfüllen, aufgrund des Vorliegens besonderer Umstände jedoch eine Freigabe zur Tätigkeit in Unterkünften für Ausländerinnen und Ausländer wegen nicht vorliegender Unbedenklichkeit von der Aufnahmekommune nicht erteilt werden konnte. Die Datenübermittlungskette auf Basis der erteilten Einwilligung der Arbeitnehmer mag, so teilte der Landesbeauftragte dem MI zusammenfassend mit, aufgrund der akuten Situation und für einen gewissen Übergangszeitraum hinnehmbar sein. Perspektivisch würde der Landesbeauftragte jedoch eine entsprechende Ergänzung des § 34a GewO vorziehen, wenn dauerhaft an der förmlichen Feststellung der Unbedenklichkeit der Beschäftigten festgehalten werden sollte.

Die Innenminister und -senatoren von Bund und Ländern hatten sich, so teilte das MI dem Landesbeauftragten mit, in einer gemeinsamen Beratung am 17. Oktober 2014 darauf verständigt, dass der Einsatz von Sicherheitspersonal in Unterkünften für Asylsuchende nur dann in Betracht komme, wenn die beauftragten Unternehmen

und Kommunen das Personal einer Zuverlässigkeits- bzw. Sicherheitsüberprüfung unterzogen hatten, die regelmäßig wiederholt wird. Ein Hinweis darauf, in welchen Zyklen diese Überprüfung wiederholt werden soll und nach welchem Verfahren, fehlte dem Erlassentwurf zunächst. Auch darauf hatte der Landesbeauftragte das MI in seiner Stellungnahme hingewiesen.

Jedoch konnte sich das MI nicht dazu entschließen, in dem letztendlich am 22. Oktober 2015 in Kraft getretenen Erlass die Hinweise des Landesbeauftragten aufzunehmen.

12.9 Reisegewerbe

Nach einer erfolgten Anmeldung eines stehenden Gewerbes finden eine ganze Reihe von Datenübermittlungen statt. Übermittelnde Stellen sind in der überwiegenden Zahl der Fälle die für die Entgegennahme der Gewerbeanzeigen zuständigen Behörden. Das sind in Sachsen-Anhalt die Gemeinden, dort in der Regel die Gewerbeämter. Rechtsgrundlage der meisten Datenübermittlungen, z. B. an die Handwerkskammern oder die Industrie- und Handelskammern, ist § 14 Abs. 8 GewO.

Der Landesbeauftragte beobachtet schon seit vielen Jahren, dass von den Gewerbeämtern ebenso wie von den Kammern übersehen wird, dass der genannte § 14 GewO lediglich „Stehende Gewerbe“ adressiert. Folglich gilt er nicht für solche Personen, die außerhalb ihrer gewerblichen Niederlassung oder ohne eine solche zu haben, die in § 55 GewO aufgeführte Tätigkeiten ausführen, also ein Reisegewerbe ausüben.

Anders als Personen, die die Aufnahme eines stehenden Gewerbes lediglich anzuzeigen haben, bedürfen Reisegewerbetreibende der behördlichen Erlaubnis (Reisegewerbekarte). Der Landesbeauftragte hat mehrfach festgestellt, dass die Gewerbeämter gelegentlich den Eingang von Anträgen auf Reisegewerbekarten nutzen, um die Antragsdaten aus den unterschiedlichsten Beweggründen heraus oder auf Basis des unzutreffenden § 14 GewO an die Kammern zu übermitteln. Betroffene beschwerten sich darüber beim Landesbeauftragten.

Zu konstatieren ist nicht nur die gewerberechtlich unzulässige Datenübermittlung von den Gewerbeämtern an die Kammern, sondern auch die unzulässige Datenerhebung durch die Entgegennahme der übermittelten Daten bei den Kammern.

Solange kein begründeter Anlass für die Annahme bei den Gewerbeämtern besteht, der Reisegewerbetreibende sei möglicherweise kammerpflichtig (weil z. B. auch handwerkliche oder handwerksähnliche Arbeiten verrichtet werden sollen), hat die Übermittlung von Daten aus den Reisegewerbekarten an die Kammern mangels Rechtsgrundlage zu unterbleiben.

12.10 Mikrozensus 2017

Das Mikrozensusgesetz (MZG) aus dem Jahr 2005 bestimmte in § 1 Abs. 1, dass in den Jahren 2005 bis 2016 über Teile der Bevölkerung und des Arbeitsmarktes sowie die Wohnsituation ausgewählter Haushalte Erhebungen als Bundesstatistik, genannt Mikrozensus, durchgeführt werden. Zweck der aufwendigen Erhebung war, statisti-

sche Angaben über die Bevölkerungsstruktur, die wirtschaftliche und soziale Lage der Bevölkerung, den Arbeitsmarkt und die Wohnverhältnisse bereitzustellen. Im Berichtszeitraum wurde ein neues MZG in Kraft gesetzt. Damit wurde angepassten Datenbedürfnissen von Bund und Ländern ebenso Rechnung getragen wie einer Reihe von Datenlieferverpflichtungen gegenüber dem Statistischen Amt der Europäischen Union (Eurostat). Dies geschah mit dem Ziel, durch zusammengefasste Erhebungen die Erhebungskosten zu dämpfen und die Belastung der Erhebungseinheiten zu verringern.

Der Landesbeauftragte hatte zu dem Gesetzentwurf gegenüber dem Ministerium für Inneres und Sport Stellung genommen und darum ersucht, die von ihm formulierten Bedenken gegen einzelne Bestimmungen im Rahmen der Länderbeteiligung zu berücksichtigen:

- Anders als im bisher geltenden § 2 Abs. 1 Satz 2 MZG 2005, der bei der Auswahl der Erhebungseinheiten von einem „mathematischen Zufallsverfahren“ spricht, lautet die entsprechende Formulierung im neuen Gesetzentwurf „mathematisch-statistisches Verfahren“.

  Falls nicht beabsichtigt ist, die Zufallskomponente bei der Auswahl der Erhebungseinheiten aufzugeben, sollte der Gesetzestext darauf explizit hinweisen, dass das Verfahren grundsätzlich zufallsgesteuert abläuft.

- Nach Erfahrungen des Landesbeauftragten bei Beratungen und der Bearbeitung von Petenteneingaben zu statistischen Fragen begegnet die Pflicht zur Angabe des Einkommens regelmäßig datenschutzrechtlichen Bedenken; das gilt selbst dann, wenn, wie im bisherigen Mikrozensusgesetz (§ 4 Abs. 1 Nr. 3 MZG 2005), eine Staffelung nach Einkommensgruppen vorgesehen ist.

  Diese Staffelung wird im neuen MZG aufgegeben. Es werden nun exakte Einkommensangaben verlangt. Eine Erforderlichkeit ist nicht erkennbar und auch der Gesetzesbegründung nicht zu entnehmen. Eine Rückkehr zu Staffelangaben scheint geboten.

- In § 8 des neuen MZG stellt sich bei einer Fülle von Merkmalen die Frage nach der Erforderlichkeit für die Zwecke der amtlichen Statistik. Vielmehr wird sich der Auskunftspflichtige in einem bisher nicht gekannten Maß durchleuchtet fühlen, z. B. bei der Erhebung der Merkmale

  - Höhe des Gewinns oder Verlustes aus selbstständiger Tätigkeit,
  - Höhe des Einkommens aus Wert- und Sparanlagen,
  - geleistete Zahlung für Grundbesitzabgaben,
  - Vorhandensein von Auto oder Computer im Haushalt,
  - rechtzeitiges Bezahlen von Mieten usw.

  Für jedes der Merkmale in § 8 Abs. 1 Nrn. 3 und 4 MZG 2016 hat der Landesbeauftragte die kritische Diskussion der Erforderlichkeit und ggf. eine ausführliche Begründung für notwendig gehalten.

Obgleich die meisten kritisierten Bestandteile des MZG europarechtlichen Vorgaben geschuldet sein dürften, gibt der Landesbeauftragte doch zu bedenken, dass nur ein von den befragten Bürgerinnen und Bürgern akzeptiertes Statistikgesetz verlässlich richtige Ergebnisse zeigen wird. Das MZG wurde im Wesentlichen unverändert beschlossen (BGBl. I 2016, S. 2826).

12.11 Zensusvorbereitungsgesetz 2021

Die Wellen, die der Zensus 2011 (vgl. XI. Tätigkeitsbericht, Nr. 12.6 und XII. Tätigkeitsbericht, Nr. 13.5) und vor allem seine Ergebnisse schlugen, haben sich noch nicht gelegt, da steht, nicht zuletzt europarechtlichen Vorgaben geschuldet, im Jahre 2021 schon die nächste große Volkszählung an. Gezählt werden wohl wieder alle Einwohner, ihr Status in Haushalt und Beruf, die Gebäude und Wohnungen, in denen sie leben, und viele andere Dinge. Es wird erwartet, dass der Zensus 2021 wieder als durch Befragungen ergänzte Registerzählung durchgeführt werden wird.

Vorhaben dieser Größenordnung bedürfen einer langfristigen und detaillierten Vorbereitung, besonders für die benötigte Infrastruktur. Den Entwurf eines entsprechenden Gesetzes (Zensusvorbereitungsgesetz 2021 – ZensVorbG 2021) hatte das Bundesministerium des Innern im Juli 2016 vorgelegt. Zu dem Gesetzentwurf, der in Teilen an das ZensVorbG 2011 angelehnt ist, konnte der Landesbeauftragte Stellung nehmen.

Wesentlicher Inhalt des ZensVorbG 2021 ist die Schaffung eines der Vorbereitung und Durchführung des Zensus 2021 dienenden Steuerungsregisters. Dieses Register enthält u. a. einen georeferenzierten Wohnanschriftenbestand und diverse Angaben zu den Auskunftspflichtigen für die Gebäude- und Wohnungszählung. Damit erscheint es in wesentlichen Teilen ein Spiegelbild des bereits bestehenden Anschriftenregisters nach § 13 Abs. 2 BStatG.

Der Landesbeauftragte brachte die folgenden Kritikpunkte vor:

- Nach § 10 Abs. 2 E-ZensVorbG 2021 dürfen die statistischen Ämter der Länder verschiedenen datenanliefernden Stellen Anschriftenbereiche mitteilen, zu denen Anhaltspunkte auf unvollständige oder fehlerhafte Daten vorliegen.

  Durch diesen Rückfluss von Informationen aus der Statistik in den Verwaltungsvollzug wird das Trennungsgebot zwischen Verwaltung und Statistik ein Stück weit aufgebrochen. Dies wäre möglicherweise noch hinnehmbar, wenn der Begriff „Anschriftenbereich“ definiert wäre. So kann nicht ausgeschlossen werden, dass sich ein Anschriftenbereich auf einen Straßenabschnitt bezieht, bei dem nur ein Gebäude existiert. Hier sollte eine datenschutz- und statistikrechtlich akzeptable Grenze vorgesehen werden.

- § 13 E-ZensVorbG 2021 enthält gegenüber § 12 ZensVorbG 2011 – Nutzung allgemein zugänglicher Quellen – eine Ergänzung dahingehend, dass zur Vorbereitung des Zensus 2021 auch Angaben aus Statistiken und statistikinternen Registern verwendet werden dürfen.

  Dies diene der Vermeidung von Doppelerhebungen und damit der Entlastung der zu Befragenden. Durch diesen Paradigmenwechsel kommt es zu einer

Vermengung von für bestimmte Statistiken erhobenen Daten, zumal wenn es sich noch um Einzelangaben handelt, ohne dass dies den einst Auskunft Erteilenden bewusst war. Das erscheint datenschutz- und statistikrechtlich zumindest fragwürdig.

- Die personenbezogenen Daten der Auskunftspflichtigen für die Erhebung an Anschriften mit Sonderbereichen und der Auskunftspflichtigen für die Gebäude- und Wohnungszählung sind nach § 16 Abs. 2 und 3 E-ZensVorbG 2021 zum frühestmöglichen Zeitpunkt, spätestens vier Jahre nach dem Zensusstichtag zu löschen. Der Anschriftenbestand nach § 4 E-ZensVorbG 2021 soll sogar erst 6 Jahre nach dem Zensusstichtag gelöscht werden.

  Erfahrungen aus der Anwendung des § 19 Abs. 1 ZensG 2011 zeigen, dass im Einzelfall mit der maximal zulässigen Speicherdauer nach dem Zensusstichtag zu rechnen sein wird. Auch vor dem Hintergrund, dass die genannten Daten ab dem Zensusstichtag keine Aktualisierung mehr erfahren, die Daten damit durch Zeitablauf teilweise falsch sind, erscheinen die Fristen zu lang.

Da das ZensVorbG 2021 auch in der Anwendungsphase der DS-GVO Wirkung entfaltet, hat der Landesbeauftragte auch geprüft, ob die Gesetzesregelungen den DS-GVO-Anforderungen entsprechen würden. Vor allem in den Blick genommen wurden die Übermittlungen von nicht zu statistischen Zwecken erhobenen und verarbeiteten Daten durch die Vermessungs- und Meldebehörden an die statistischen Landesämter. Die Weiterverarbeitung dieser Daten zu statistischen Zwecken wäre nach Art. 5 Abs. 1 lit. b DS-GVO i. V. m. Art. 89 Abs. 1 DS-GVO mit ihren ursprünglichen Zwecken vereinbar. Auch die Löschpflichten nach Art. 17 DS-GVO werden eingehalten.

Leider konnten sowohl der Landesbeauftragte als auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit ihren Vorschlägen nicht durchdringen. Die zweifelhaften Formulierungen sind Gesetzestext geworden (ZensVorbG 2021, BGBl. I 2017, S. 388).

12.12 Telearbeit für eine kommunale Statistikstelle

Eine Möglichkeit, die Vereinbarkeit von Familie und Beruf zu fördern, ist die Teleheimarbeit. Dabei werden mittels geeigneter IT-Verfahren Arbeitsleistungen, die bisher eher in Unternehmen oder Behörden erbracht wurden, in den heimischen Bereich verlagert. Allerdings ist dies kein Grund, bei der Verarbeitung personenbezogener oder geheim zu haltender Daten Regelungen des Datenschutzes und der Geheimhaltung unberücksichtigt zu lassen. Es birgt Risiken, wenn personenbezogene Daten die verantwortliche Stelle verlassen, um an einem anderen Ort bearbeitet zu werden. Der Landesbeauftragte hatte sich dazu bereits in seinem IX. Tätigkeitsbericht (Nr. 14.14) geäußert.

Im Berichtszeitraum hatte er sich aufgrund einer Anfrage damit zu befassen, ob es grundsätzlich auch zulässig sein könnte, für eine kommunale Statistikstelle im Sinne von § 7 StatG-LSA Teleheimarbeit zu leisten und was dabei ggf. zu beachten wäre.

Der Landesbeauftragte vertritt vor dem Hintergrund der für kommunale Statistikstellen in Sachsen-Anhalt geltenden Geheimhaltungsvorschriften des StatG-LSA den Standpunkt, dass grundsätzliche Hinderungsgründe, für eine kommunale Statistik-

stelle auch an einem Teleheimarbeitsplatz tätig zu sein, nicht bestehen. Im Besonderen in § 7 StatG-LSA, der die kommunalen Statistikstellen und besonders die räumliche, organisatorische und personelle Trennung vom übrigen Verwaltungsvollzug regelt, und in § 14 StatG-LSA, der Vorschriften über das Statistikgeheimnis beinhaltet, sind solche Hinderungsgründe nicht ersichtlich. Folgendes ist jedoch zu beachten:

Unterlagen mit nach statistik- oder datenschutzrechtlich vertraulich zu behandelnden Merkmalen (Einzelangaben) dürfen nicht zum Heimarbeitsplatz mitgenommen werden.

Aber auch an die zu verwendende IT sind strenge Anforderungen zu stellen. So dürfen ausschließlich von der die Teleheimarbeit genehmigenden Behörde bereitgestellte Computer bzw. Laptops verwendet werden. Die Nutzung privater Hardware ist ausgeschlossen. Für den Anschluss des Gerätes an das Verwaltungsnetz der Behörde darf ausschließlich der von der IT-Abteilung vorgesehene Übertragungsweg verwendet werden, bei Nutzung des öffentlichen Kommunikationsnetzes hat dies durch geeignete Verschlüsselung über ein virtuelles privates Netz zu erfolgen. Andere Netzwerkfunktionalitäten, wie z. B. das WLAN, sind abzuschalten.

Notwendige Voraussetzung ist weiterhin, dass es dem Nutzer des Gerätes technisch unmöglich ist, auf den lokalen Datenträgern seines Gerätes vertrauliche Angaben zu speichern. Dazu sind die Nutzerrechte auf das absolut notwendige Maß zu beschränken. Das gilt auch für den Zugriff auf die Betriebssystemebene.

Die Nutzung von Druckern, von USB-Speichergeräten und von in- und externen Schreibgeräten für optische Datenträger (CD/DVD-Brenner) ist technisch auszuschließen.

Für weniger relevant hält der Landesbeauftragte dagegen gelegentlich erhobene Forderungen nach der Abschließbarkeit des häuslichen Arbeitszimmers bzw. danach, dass dieses Zimmer nur für den Heimarbeitenden zugänglich sein soll. Die Erfüllung dieser Forderungen ist schlicht nicht überprüfbar. Hat der Heimarbeitende sich von der dienstlichen Software abgemeldet und den VPN-Tunnel geschlossen, und dazu ist er für jeden Fall des Verlassens des heimischen Arbeitszimmers zu verpflichten, existiert kein Heimarbeitsplatz mehr.

Jedoch machte der Landesbeauftragte auf einen weiteren organisatorischen Aspekt aufmerksam: Nach § 7 Abs. 3 StatG-LSA hat der Bürgermeister die nach dem Gesetz erforderlichen Maßnahmen der räumlichen, organisatorischen und personellen Trennung der kommunalen Statistikstelle vom Verwaltungsvollzug in einer schriftlichen Dienstanweisung festzulegen. In diese Dienstanweisung dürften zur Gewähr transparenten Verwaltungshandelns auch die Bedingungen gehören, unter denen Heimarbeit für die Statistikstelle zugelassen ist. Dies gilt auch für die nach § 7 Abs. 5 StatG-LSA erforderliche ortsübliche Bekanntmachung der Einrichtung einer kommunalen Statistikstelle und für die entsprechenden Anzeigen gegenüber dem Statistischen Landesamt, der Kommunalaufsichtsbehörde und dem Landesbeauftragten für den Datenschutz.

Bei zukünftigen Kontrollen kommunaler Statistikstellen wird der Landesbeauftragte auch die Einrichtung möglicher Teleheimarbeitsplätze zu prüfen haben.

13 Wirtschaft

13.1 Düsseldorfer Kreis

Bereits unter Nr. 14.1 des XII. Tätigkeitsberichts wurden die Ziele und die Arbeitsweisen des Düsseldorfer Kreises der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) vorgestellt. Im Berichtszeitraum hat der Düsseldorfer Kreis u. a. folgende Beschlüsse gefasst:

- Beschluss vom März 2016: Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen[8]

  Diese Orientierungshilfe enthält Hinweise zur datenschutzgerechten Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen nach § 4a BDSG und elektronischen Texten nach § 13 Abs. 2 und Abs. 3 TMG.

- Beschluss vom 13. und 14. September 2016: Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung (**Anlage 25**)

  In dem Beschluss wird erläutert, dass Einwilligungen, die nach § 4a BDSG eingeholt wurden, unter bestimmten Voraussetzungen auch unter der DS-GVO fortgelten können. Dies gilt aber nur dann, wenn die Alteinwilligungen den Bedingungen der DS-GVO entsprechen.

Darüber hinaus waren der Düsseldorfer Kreis und seine Arbeitsgruppen mit der Vorbereitung auf die DS-GVO und das BDSG 2018 befasst. Unter deren Mitwirkung sind die Kurzpapiere der DSK zu wesentlichen Themen der DS-GVO erarbeitet worden (s. Homepage des Landesbeauftragten). Die Umstellung auf die DS-GVO und das BDSG 2018 wird auch die weitere Arbeit wesentlich bestimmen. Eine Vielzahl von Orientierungshilfen und Beschlüssen bedürfen der Anpassung.

Der Düsseldorfer Kreis – der fortan als „Arbeitskreis Wirtschaft“ der DSK fungiert – wird infolge der maßgeblichen, verbindlichen Auslegungen des Datenschutzrechts seine erhebliche Bedeutung für den nichtöffentlichen Bereich beibehalten. Aber auch die Hinweise aus den Facharbeitskreisen, zu denen die Arbeitsgruppen des Düsseldorfer Kreises aufgewertet wurden, sind ebenso zu beachten.

13.2 Datenschutzmanagement – DS-GVO und BDSG 2018

Mit voranschreitender Zeit spielte für den Landesbeauftragten zunehmend die Vorbereitung auf die DS-GVO und das BDSG 2018 eine wesentliche Rolle. Es galt, den Verantwortlichen – insbesondere deren Geschäftsleitungen – frühzeitig Informationen bereit zu stellen. Bei der Anpassung des betrieblichen Datenschutzmanagements an die DS-GVO und das BDSG 2018 ist insbesondere Folgendes zu beachten:

[8] http://lsaurl.de/OHEinwillForm

Datenschutz als Querschnittsaufgabe betrifft unterschiedliche betriebliche Bereiche. Anwenden müssen ihn alle Mitarbeiter, die personenbezogene Daten verarbeiten. Dies können z. B. Bürokräfte, Sachbearbeiter, Kundenberater oder IT-Verantwortliche sein, die – untereinander abgestimmt – für eine datenschutzgerechte Verarbeitung zu sorgen haben. Da regelmäßig unterschiedliche betriebliche Bereiche betroffen sind, ist der Datenschutz eine Aufgabe des Managements und damit Chefsache. Dies gilt insbesondere in Bezug auf die Anwendung von DS-GVO und BDSG 2018. Die **Geschäftsleitung** trägt hier die Gesamtverantwortung für das Unternehmen. Sie muss die organisatorischen Voraussetzungen dafür schaffen, dass die neuen datenschutzrechtlichen Vorgaben im Unternehmen umgesetzt werden. Dies beinhaltet die Erteilung von Weisungen genereller Art, bei schwierigen Sachverhalten auch im Einzelfall. Weiterhin müssen die unternehmensinternen Zuständigkeiten festgelegt werden. Erforderlich ist es, die **Beschäftigten**, die personenbezogene Daten verarbeiten, auch weiterhin auf die Einhaltung des Datenschutzes zu verpflichten. Ferner muss durch die Geschäftsleitung geprüft werden, ob ein **Datenschutzbeauftragter** zu bestellen ist. Sie muss die finanziellen, sachlichen und personellen Ressourcen bereitstellen, die für die Einhaltung des Datenschutzes erforderlich sind. Dazu gehört auch die Schulung der Mitarbeiter. Sie muss sicherstellen, dass die Einhaltung des Datenschutzes angemessen überwacht wird. Vor diesem Hintergrund muss die Leitung dafür Sorge tragen, dass jedenfalls die folgenden Aufgaben bewältigt werden:

Alle Beschäftigten, die personenbezogene Daten verarbeiten, sind auf die Neuerungen der DS-GVO und des BDSG 2018 sowie bereits in Kraft getretener Spezialregelungen hinzuweisen. Um den betrieblichen Anpassungsbedarf an die neuen Vorschriften zu ermitteln, sollte eine Bestandsaufnahme durchgeführt werden, inwieweit bei gegenwärtigen Prozessen personenbezogene Daten verarbeitet werden.

Da auch unter der DS-GVO eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten erforderlich ist, sollte sodann geprüft werden, ob das neue Recht für alle derzeitigen Verarbeitungen eine Rechtsgrundlage (Art. 6 bis 11 DS-GVO) bereitstellt bzw. ob noch Prozesse der Rechtslage angepasst werden müssen. Besondere Beachtung ist der Verarbeitung der Daten von Kindern zu widmen (Art. 6 Abs. 1 lit. f und Art. 8 DS-GVO).

Die DS-GVO enthält Regelungen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO). Schon bei Prozess- und Produktentwicklung ist durch die Geschäftsleitung darauf hinzuwirken, wie die Datenschutzgrundsätze – etwa die Datenminimierung – umgesetzt werden können. Durch Voreinstellungen in Hardware- und Software-Produkten muss gewährleistet sein, dass nur solche personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Verträge, die die Verarbeitung personenbezogener Daten betreffen, sollten überprüft und ggf. angepasst werden, soweit dies noch nicht geschehen ist. Im Falle der gemeinsamen Verarbeitung mehrerer Verantwortlicher wäre insbesondere Art. 26 und bei der Auftragsverarbeitung wären insbesondere die Art. 27 und 28 DS-GVO zu beachten. Auch Betriebsvereinbarungen und Tarifverträge sollten unter Berücksichtigung des BDSG 2018 geprüft werden.

Die bisher durchzuführende Vorabkontrolle (s. § 4d Abs. 5 BDSG) wird abgelöst durch die Datenschutz-Folgenabschätzung (DSFA). Die Geschäftsleitung muss dafür

Sorge tragen, dass sie immer dann durchgeführt wird, wenn eine Form der Verarbeitung ein hohes Risiko für die betroffene Person zur Folge hat (Art. 35 Abs. 1 DS-GVO). Sie ist insbesondere erforderlich bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten, z. B. Gesundheitsdaten, oder bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (vgl. ErwGr 84, 90-93 DS-GVO und Kurzpapier Nr. 5 der DSK). Eine vorläufige Liste von Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist, befindet sich auf der Homepage des Landesbeauftragten. Geht aus der DSFA hervor, dass die Verarbeitung ein hohes Risiko hat und trifft der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos, so muss durch die Geschäftsleitung sichergestellt werden, dass die Aufsichtsbehörde konsultiert wird (Art. 36 DS-GVO).

Weiterhin muss gewährleistet werden, dass die Rechte der betroffenen Personen gewahrt werden (Art. 12 bis 22 DS-GVO). Die Betroffenenrechte haben in der DS-GVO wesentliche Veränderungen erfahren. Gänzlich neu sind das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit.

Hat der Verantwortliche zu löschende Daten zuvor öffentlich bekannt gemacht, muss er angemessene Maßnahmen treffen, um die Verantwortlichen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person Löschung verlangt hat (Art. 17 DS-GVO).

Nach dem Recht auf Datenübertragbarkeit müssen personenbezogene Daten auf Antrag der betroffenen Person ihm oder einem anderen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, wenn die Verarbeitung automatisiert erfolgt und auf Einwilligung oder Vertrag nach Art. 6 Abs. 1 lit. b DS-GVO beruht.

Zudem hat der Betroffene das Recht, in besonderen Situationen der Verarbeitung zu widersprechen, welche u. a. auf einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO beruhen (gilt auch für Profiling). Folge des Widerspruchs ist, dass keine Weiterverarbeitung zulässig ist, es sei denn, das Überwiegen zwingender schutzwürdiger Gründe kann nachgewiesen werden oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Wesentlich erweitert wurden die Informationspflichten (Art. 13, 14 DS-GVO), die ab der Erhebung personenbezogener Daten zu erfüllen sind. Insbesondere Datenschutzerklärungen sind hier zu überprüfen.

Intensiviert gegenüber der derzeitigen Rechtslage wurden auch Dokumentations-, Nachweis- und Meldepflichten.

Abgesehen von seltenen Ausnahmen für einzelne Kleinbetriebe muss vom Verantwortlichen und Auftragsverarbeiter (nicht mehr vom Datenschutzbeauftragten) ein Verzeichnis von Verarbeitungstätigkeiten geführt werden, welches der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist (Art. 30 DS-GVO). Ein Vordruck befindet sich auf der Homepage des Landesbeauftragten.

Ansprechpartner für die Aufsichtsbehörde ist beim Verantwortlichen und beim Auftragsverarbeiter der jeweilige Datenschutzbeauftragte (vgl. § 40 Abs. 6 Satz 1 BDSG 2018). Dieser ist bei nichtöffentlichen Stellen gem. § 38 Abs. 1 Satz 1 BDSG 2018 zu

benennen, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten. Darüber hinaus ist gem. Satz 2 dieser Vorschrift ein Datenschutzbeauftragter u. a. dann zu benennen, wenn eine DSFA durchzuführen ist. Nach Art. 37 Abs. 1 DS-GVO gilt diese Pflicht auch, wenn die Kerntätigkeit eines Unternehmens in der systematischen Überwachung von Personen oder in der Verarbeitung besonderer Kategorien von Daten liegt (Art. 9 DS-GVO).

Der Unternehmer ist für die Einhaltung der Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) im Rahmen der Rechenschaftspflicht nachweispflichtig (Art. 5 Abs. 2 DS-GVO).

13.3 Auskunftspflicht gegenüber der Aufsichtsbehörde

Das VG Magdeburg hat bezüglich einer Klage gegen einen Auskunftsbescheid des Landesbeauftragten die Auskunftspflicht nach § 38 Abs. 3 Satz 1 BDSG konkretisiert (Urteil vom 14. November 2016, Az. 1 A 288/16 MD). Die Rechtslage ist insoweit auch nach der DS-GVO und dem BDSG 2018 unverändert. Das Gericht stellte klar, dass die Auskunftspflicht nicht erfüllt ist, wenn dem Landesbeauftragten lediglich Unterlagen oder Schriftsätze aus anderen gerichtlichen Verfahren übersandt werden, aus denen er sich die erfragten Angaben selber heraussuchen muss. Vielmehr besteht die Auskunftspflicht nach Ansicht des VG Magdeburg darin, die in einem Auskunftsbescheid gestellten Fragen auch konkret beantworten zu müssen. Das OVG Sachsen-Anhalt hat den Antrag des Klägers auf Zulassung der Berufung zurückgewiesen und folgte ganz überwiegend den wesentlichen Gründen des VG Magdeburg (OVG Sachsen-Anhalt, Beschluss vom 9. November 2017, Az. 3 L 54/17.Z). Das OVG Sachsen-Anhalt führte insbesondere aus: „Es ist weder Sache der Datenschutzbehörde noch des Verwaltungsgerichts, sich aus dem Verwaltungsvorgang die notwendigen „Angaben und Unterlagen“ herauszusuchen oder aus Schriftsätzen, die Gegenstand eines zivilgerichtlichen Rechtsstreits gewesen sind, dasjenige herauszufiltern, was möglicherweise zur Beantwortung der gestellten Fragen geeignet sein könnte.“ Die Auskunftspflicht nach § 38 Abs. 3 Satz 1 BDSG erstreckte sich auf alle Angaben, die die Aufsichtsbehörde zur Erfüllung ihrer Aufgaben benötigt. Hiervon umfasst ist die Pflicht zur Erteilung von Auskünften, die der Aufsichtsbehörde die Beurteilung ermöglichen soll, ob überhaupt ein Sachverhalt vorliegt, auf den das BDSG Anwendung findet. Die verlangten Auskünfte müssen der Aufsichtsbehörde ohne schuldhaftes Zögern, vollständig und wahrheitsgemäß erteilt werden.

Mit Geltung der DS-GVO seit dem 25. Mai 2018 können die Aufsichtsbehörden den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und ggf. den Vertreter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters gemäß Art. 58 Abs. 1 lit. a DS-GVO anweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind.

13.4 Meldepflicht bei Datenpannen

Nach § 42a BDSG und § 15a TMG hatten nichtöffentliche Stellen die Pflicht zur Anzeige an den Landesbeauftragten als zuständige Aufsichtsbehörde, wenn sie fest-

stellten, dass bestimmte bei ihnen gespeicherte Daten Dritten unrechtmäßig zur Kenntnis gelangt sind. § 42a BDSG betraf personenbezogene Daten besonderer Art (§ 3 Abs. 9 BDSG), Daten, die einem Berufsgeheimnis unterliegen, Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den diesbezüglichen Verdacht beziehen oder Daten zu Bank- und Kreditkartenkonten. § 15a TMG bezog sich auf Datenpannen bei Diensteanbietern von Telemedien im Zusammenhang mit Bestandsdaten (z. B. Name und Adresse) oder Nutzungsdaten (z. B. Login-Daten wie User-ID oder Passwort). Weitere Voraussetzung der Anzeigepflichten war, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Für die Datenverarbeitung verantwortliche Unternehmen mussten bei Datenpannen eine Gefahrenprognose vornehmen, die Frage erheblicher materieller oder sozialer Schäden prüfen und die Eintrittswahrscheinlichkeit ermitteln. Bei Vorliegen der Voraussetzungen waren weitere Handlungen geboten, z. B. Maßnahmen zur Minderung nachteiliger Folgen und die Benachrichtigung der Betroffenen. Die Benachrichtigung der Aufsichtsbehörde musste nach § 42a Satz 4 BDSG eine Darlegung möglicher nachteiliger Folgen des Abhandenkommens der Daten und der vom Betreiber nach dem Abhandenkommen ergriffenen Maßnahmen enthalten.

Die dem Landesbeauftragten im Berichtszeitraum gemeldeten Datenpannen zeigten einmal mehr, wie wichtig sorgfältiger Umgang mit personenbezogenen Daten auch bei vermeintlich harmlosen Alltagsvorgängen ist.

So kam es in einem gemeldeten Fall vor, dass ein Brief mit Kontoauszügen durch eine Bank an einen Unberechtigten gesandt wurde; es bestand Namensgleichheit mit dem berechtigten Empfänger. In einem anderen Fall wurden Bankunterlagen über Sparguthaben an einen unberechtigten Empfänger verschickt; ein Bankmitarbeiter hatte die Papiere versehentlich mit in den falschen Briefumschlag gesteckt.

Im Falle des Versands von Unterlagen mit personenbezogenen Daten an Unberechtigte rät der Landesbeauftragte grundsätzlich dazu, vom Unberechtigten die Herausgabe der Unterlagen zu verlangen, sofern diese noch nicht vernichtet sind, und den Unberechtigten darauf hinzuweisen, dass er zu keiner Verarbeitung oder Nutzung der Daten befugt ist.

In anderen Fällen verschafften sich Personen durch Einbruch in Gebäude oder durch die Verwendung von rechtswidrig erlangten Zugangsdaten zu elektronischen Schließfächern Zugriff auf personenbezogene Daten.

In einem weiteren Fall wurde eine Datenbank bei einem Dienstleister von Banken angegriffen. Dabei erfolgte ein Datenzugriff auf Kontaktdaten von Mitarbeitern und Kunden von Banken.

Nicht alle eingegangenen Meldungen zu § 42a BDSG wurden vom Landesbeauftragten so eingeschätzt, dass tatsächlich eine Benachrichtigungspflicht bestand. Dies lag insbesondere daran, dass im Einzelfall keine schwerwiegenden Beeinträchtigungen drohten. Der Landesbeauftragte rät gleichwohl, ihn auch in Zweifelsfällen zu informieren. Das Risiko einer fehlerhaften Prognose trägt die verantwortliche Stelle.

Die Anforderungen an die Erfüllung der Meldepflicht bei Datenpannen sind durch die Art. 33 und 34 DS-GVO seit dem 25. Mai 2018 deutlich erweitert worden:

Die Meldung an die Aufsichtsbehörde muss gemäß Art. 33 Abs. 1 DS-GVO unverzüglich und möglichst binnen 72 Stunden, nachdem dem Verantwortlichen die Verletzung (Art. 4 Nr. 12 DS-GVO) bekannt wurde, erfolgen. Eine Verzögerung bedarf der Begründung. Grundsätzlich ist jede Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden – unabhängig von den betroffenen Datenarten. Eine Ausnahme gilt bei voraussichtlich fehlendem Risiko. Auch die Dokumentationspflicht ist erweitert worden (Art. 33 Abs. 5 DS-GVO).

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich sogar ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, hat gemäß Art. 34 Abs. 1 DS-GVO grundsätzlich eine Benachrichtigung der Betroffenen zu erfolgen. Inhaltlich muss die Benachrichtigung zumindest die in Art. 33 Abs. 3 lit. b, c und d DS-GVO genannten Informationen und Maßnahmen enthalten.

13.5 Personalausweiskopie

Immer häufiger wird von Kunden – beispielsweise bei Einkäufen über das Internet – die Überlassung einer Personalausweiskopie gefordert. Der Landesbeauftragte hatte dieses Thema schon mehrfach aufgegriffen (XI. Tätigkeitsbericht, Nr. 13.2.2; XII. Tätigkeitsbericht, Nr. 14.6).

Das Fotokopieren, Fotografieren und Einscannen von Personalausweisen ist neuerdings ausdrücklich geregelt. Mit Wirkung vom 18. Juli 2017 wurde das PAuswG geändert. Nach dem neuen § 20 Abs. 2 PAuswG darf der Ausweis „abgelichtet“ werden. Dies aber nur mit Einwilligung des Ausweisinhabers und auch nur dann, wenn die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Nur der Ausweisinhaber entscheidet darüber, ob er überhaupt personenbezogene Daten durch Ablichtung seines Ausweises preisgeben will und in welchem Umfang dies erfolgt (§ 20 Abs. 2 Satz 3 PAuswG). Seine Einwilligung muss freiwillig und grundsätzlich schriftlich erfolgen. Zuvor muss der Ausweisinhaber auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten hingewiesen werden. Außerdem hat er das Recht zur Unkenntlichmachung (z. B. Schwärzung) derjenigen personenbezogenen Daten, die er nicht preisgeben will. Für Pässe gelten inhaltlich identische Vorschriften (§ 18 Abs. 3 PassG).

Die Kopie eines Personalausweises ohne Einwilligung ist zulässig, wenn eine gesetzliche Vorschrift das Kopieren ausdrücklich erlaubt oder sogar vorschreibt. Zur Fertigung von Personalausweiskopien durch die Kreditwirtschaft siehe Nr. 13.6.

13.6 Kreditwirtschaft

Fotokopien von Personalausweisen zur Identifizierung natürlicher Personen

Nach bisheriger Rechtslage konnten auch im Bereich der Kreditwirtschaft Fotokopien von Personalausweisen nur gefertigt werden, wenn die für den Zweck der Identifizierung nicht erforderlichen Daten z. B. durch Nutzung einer Schablone zuvor abgedeckt wurden. Nunmehr haben die nach dem Geldwäschegesetz (GwG) Verpflichteten „das Recht und die Pflicht, vollständige Kopien dieser Dokumente oder Unterlagen anzufertigen oder sie vollständig optisch digitalisiert zu erfassen“ (§ 8 Abs. 2

Satz 2 GwG), soweit dies zur Überprüfung der Identität einer natürlichen Person erforderlich ist.

Videoidentifizierung

Nach § 11 Abs. 1 GwG sind die Kredit- und Finanzdienstleistungsinstitute verpflichtet, Vertragspartner – z. B. im Falle einer Kontoeröffnung – zu identifizieren. Bankkunden, die z. B. online ein Konto eröffnen möchten, können diese Identifizierung per Videochat durchführen lassen. Dazu bedarf es einer leistungsfähigen Internet-Verbindung, einer Webcam sowie eines Ausweispapiers. Zentraler Bestandteil der Videoidentifizierung ist die Prüfung der Echtheit der Ausweispapiere, i. d. R. des Personalausweises. Die Ausweise werden per Screenshot abgelichtet. Dem Kunden wird eine Transaktionsnummer (TAN) übermittelt, die er online eingeben muss.

Diese Videoidentifizierung kann datenschutzrechtlich zulässig sein. Dazu bedarf es allerdings der freiwilligen und informierten Einwilligung des Vertragspartners, bevor Daten mithilfe des Videochats erhoben und gespeichert werden. Es dürfen nur die Daten erhoben werden, die für die Identifikation erforderlich sind. Bei Störungen, z. B. bei Erscheinen unbeteiligter Personen im Erfassungsbereich, ist der Chat abzubrechen und zeitnah zu löschen. Erforderlich ist zudem eine hochwertige Verschlüsselung, die eine Kenntnisnahme Unberechtigter ausschließt. Zudem sollte zur Übermittlung der TAN ein anderes Gerät genutzt werden, als dasjenige, mit dem die Videoidentifikation durchgeführt wird.

Identifizierungspflichten auch für die für den Vertragspartner auftretenden Personen

Nunmehr bestehen auch Identifizierungspflichten für Boten und Bevollmächtigte des Vertragspartners. Diese wurden durch das „Gesetz zur Umsetzung der Richtlinie über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten sowie den Zugang zu Zahlungskonten mit grundlegenden Funktionen“ in das GwG aufgenommen (BGBl. I 2016, S. 720).

13.7 Versicherungswirtschaft

Unzulässige Verarbeitung zu Werbezwecken

Versicherungsvertreter verfügen häufig über unterschiedliche Datenbanken. Eine Datenbank dient der Begründung, Durchführung oder Beendigung von Versicherungsverträgen. Die Erhebung, Speicherung, Veränderung oder Übermittlung personenbezogener Daten in bzw. aus dieser Datei war nach § 28 Abs. 1 BDSG immer dann zulässig, wenn es für die Begründung, Durchführung oder Beendigung des Versicherungsvertrages erforderlich war.

Eine weitere Datenbank ist die sog. „Akquise-Datenbank“. Hier werden personenbezogene Daten von Personen gespeichert, die vom Versicherungsvertreter beworben werden sollen. Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten in dieser Datenbank richtete sich nicht nach § 28 Abs. 1 BDSG, sondern nach § 28 Abs. 3 BDSG. Danach war die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung zulässig, soweit der Betroffene eingewilligt hatte oder es sich um listenmäßig oder sonst zusammengefasste Daten

handelte. Diesen Listendaten konnten E-Mailadressen hinzugespeichert werden, wenn sie im Rahmen einer Geschäftsbeziehung erhoben wurden.

Im Rahmen einer zu prüfenden Beschwerde wurde festgestellt, dass ein Versicherungsvertreter in der Akquise-Datenbank gespeicherte Daten einer betroffenen Person nutzte, um Werbung per E-Mail zuzusenden, obwohl zu ihr über den Zeitraum von über fünf Jahren kein Kontakt bestand. Selbst wenn es ursprünglich aufgrund einer Einwilligung oder zur Begründung eines Versicherungsvertrages zulässig gewesen wäre, die E-Mailadresse der betroffenen Person zu erheben und zu speichern, kam eine Nutzung der Daten nach 5 Jahren nicht mehr in Betracht. Einwilligungen werden nicht stets auf unbegrenzte Dauer erteilt. So hat das Landgericht München I im Urteil vom 8. April 2010 (Az. 17 HK O 138/10) entschieden, dass eine Einwilligung zur E-Mail-Werbung nach 17 Monaten ihre Aktualität verliert und keine Rechtsgrundlage mehr für Werbung ist. Für den Fall der Nutzung von Listendaten nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG standen der Nutzung nach mehr als fünf Jahren schutzwürdige Interessen der betroffenen Person entgegen (§ 28 Abs. 3 Satz 6 BDSG).

Bei der Bearbeitung des Sachverhalts stellte der Landesbeauftragte weiterhin fest, dass bei der genannten werblichen Ansprache auch die nach § 28 Abs. 4 Satz 2 BDSG stets erforderliche Unterrichtung über das Recht zum Werbewiderspruch unterlassen wurde und auch die nach § 34 BDSG verlangte Auskunft zunächst verweigert wurde.

Die drei genannten Verstöße gegen das BDSG stellten Ordnungswidrigkeiten dar, weshalb in der Sache ein Bußgeldbescheid erging.

Verhaltensregeln

Für die Verarbeitung personenbezogener Daten in der Versicherungswirtschaft gibt es bereits seit dem Jahr 2013 Verhaltensregeln des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) für den Umgang mit personenbezogenen Daten, auch Code of Conduct genannt. In diesem Code of Conduct verpflichteten sich die angeschlossenen Versicherungsunternehmen, die darin niedergelegten Vorgaben einzuhalten. Rechtsgrundlage für diese Verhaltensregeln war § 38a BDSG und ist nunmehr Art. 40 DS-GVO.

Aufgrund der anzuwendenden DS-GVO wurden die ursprünglichen Verhaltensregeln überarbeitet, ohne dass es zu einer Genehmigung einer Aufsichtsbehörde i. S. v. Art. 40 Abs. 5 DS-GVO kam. Diese internen Verhaltensregeln wurden aber den Aufsichtsbehörden vom GDV zur Kenntnis gegeben. Versicherungsunternehmen, die diese Regeln anwenden, stellen damit sicher, dass die Vorgaben der DS-GVO für die Versicherungswirtschaft als konkretisiert gelten.

Art. 7 Abs. 3 Satz 3 DS-GVO verlangt, dass eine Einwilligung zur Verarbeitung personenbezogener Daten mit einer Belehrung über die Widerrufsmöglichkeit der Einwilligung zu versehen ist. Dies hatten die früheren Verhaltensregeln des GDV bereits vorweggenommen. Sofern sich Versicherungsunternehmer, -makler und -vertreter an diese Regelung gehalten haben, würden sich daher nachträgliche Belehrungen über die Widerrufsmöglichkeit erübrigen.

Auskünfte an Staatsanwaltschaften

Mehrfach erhielt der Landesbeauftragte Anfragen eines Versicherungsunternehmens, inwieweit personenbezogene Daten an Staatsanwaltschaften übermittelt werden dürfen. Die jeweiligen Ersuchen der Staatsanwaltschaft enthielten lediglich den Hinweis, dass ein Ermittlungsverfahren eingeleitet worden sei, und den Tatvorwurf. Ermächtigungsgrundlagen, auf die die Ersuchen gestützt worden waren, wurden nicht benannt.

Die Übermittlung personenbezogener Daten zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten war nach § 28 Abs. 2 Nr. 2. b) BDSG nur zulässig, wenn kein Grund zu der Annahme bestand, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hatte. Schutzwürdige Interessen schlossen die Übermittlung aus. Die verantwortlichen Stellen mussten daher alle Informationsmöglichkeiten nutzen, um die Voraussetzungen des § 28 Abs. 2 Nr. 2. b) BDSG zu prüfen. Dies schloss auch Nachfragen bei der anfragenden Staatsanwaltschaft ein.

Ergänzend zu einer Beratung des Versicherungsunternehmens hat der Landesbeauftragte die Staatsanwaltschaft gebeten, bei Auskunftsersuchen an Unternehmen die Ermächtigungsgrundlage anzugeben bzw. die Tatsachen zu benennen, die der verantwortlichen Stelle eine Prüfung der schutzwürdigen Interessen ermöglichen. Der schlichte Hinweis auf die Durchführung eines Ermittlungsverfahrens unter Nennung des Tatvorwurfs reicht regelmäßig nicht aus, eine solche Prüfung durchzuführen.

Auch nach der neuen Rechtslage gem. § 24 Abs. 1 BDSG 2018 ist die Verarbeitung personenbezogener Daten zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten nur zulässig, sofern dies erforderlich ist und die Interessen der betroffenen Person am Ausschluss der Verarbeitung nicht überwiegen.

13.8 Auskunfteien

Nach alter Rechtslage waren die datenschutzrechtlichen Voraussetzungen für die Tätigkeit der Auskunfteien in den §§ 28a, 28b und 29 BDSG geregelt, wobei § 28a die Datenübermittlung an Auskunfteien regelte. Mittlerweile ist Grundlage für die Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Die entsprechende Einmeldung erfordert, dass sie zur Wahrnehmung der berechtigten Interessen des Einmeldenden oder eines Dritten erforderlich ist und Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Die Prüfung dieser Voraussetzungen muss einzelfallbezogen erfolgen. Gleichwohl entfalten bestimmte Fallgruppen eine Indizwirkung für die Zulässigkeit der Einmeldung. Diese Fallgruppen betreffen titulierte oder unbestrittene Forderungen, diese sind im Beschluss der DSK vom 23. März 2018 („Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO“, **Anlage 22**) näher beschrieben.

Ein weiterer Beschluss der DSK bezieht sich auf die Unzulässigkeit fortlaufender Bonitätsauskünfte an den Versandhandel. Bonitätsauskünfte durch Auskunfteien sind ebenfalls nur im Falle des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig. Zwar können im Falle von Dauerschuldverhältnissen fortlaufende Bonitätsauskünfte mitunter statt-

haft sein. Ein Versandhandelsgeschäft stellt jedoch kein Dauerschuldverhältnis dar, selbst wenn ein Kundenkonto eingerichtet wurde. Ein berechtigtes Interesse des Versandhandels an einer Bonitätsauskunft besteht nur, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko besteht (Beschluss der DSK vom 23. März 2018 „Keine fortlaufenden Bonitätsauskünfte an den Versandhandel“, **Anlage 23**).

Mit der Frage, inwieweit Positivdaten – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – durch Auskunfteien verarbeitet werden können, hat sich die DSK ebenfalls befasst. Bei Verträgen, die eine einmalige Leistung zum Gegenstand haben, ist die Erhebung dieser Daten durch die Auskunfteien regelmäßig unzulässig, es sei denn, es liegt eine Einwilligung nach Art. 7 DS-GVO vor.

Eine Ausnahme besteht für den Bereich der Kreditinstitute. Diese unterliegen besonderen Bonitätsprüfungspflichten. Die Aufsichtsbehörden sehen es hier im Rahmen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO als zulässig an, wenn Daten über die Begründung, die ordnungsgemäße Durchführung und Beendigung von Kredit- und Giroverträgen sowie Garantiegeschäften an Auskunfteien übermittelt werden. Dies gilt allerdings nur, sofern nicht die Interessen der betroffenen Personen am Ausschluss der Übermittlung überwiegen (Beschluss der DSK vom 11. Juni 2018, „Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien“, **Anlage 24**).

13.9 Werbung

Verkaufsförderung und Imagepflege können sicherlich in vielen Fällen den wirtschaftlichen Erfolg von Unternehmen entscheidend beeinflussen. Die rechtlichen Vorgaben für den Umgang mit personenbezogenen Daten zu Werbezwecken werden allerdings nicht immer vollständig beachtet. Der Landesbeauftragte hat auch schon in seinem XI. Tätigkeitsbericht (Nrn. 13.2.4; 13.2.5; 13.4.1; 13.4.2) und XII. Tätigkeitsbericht (Nr. 14.11) über Defizite berichtet. Den Landesbeauftragten erreichten weiterhin mehrere Beschwerden über Werbung. Häufig ging es dabei um unzulässige Werbung per E-Mail.

Die Werbung per E-Mail ist gegenüber Neukunden nur zulässig, wenn eine ausdrückliche Einwilligung vorliegt (§ 7 Abs. 2 Nr. 3 UWG). Bei den Bestandskunden ist E-Mail-Werbung zulässig, wenn die E-Mail-Adresse des Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erlangt wurde, ausschließlich für eigene ähnliche Waren oder Dienstleistungen geworben wird, dem bisher nicht widersprochen wurde und bei Erhebung der E-Mail-Adresse und bei jeder Werbung erneut auf das Widerspruchsrecht hingewiesen wird (§ 7 Abs. 3 UWG).

Einwilligungen sind mitunter nur für einen begrenzten Zeitraum aktuell und damit auch nur begrenzt als Grundlage für die Verarbeitung personenbezogener Daten heranzuziehen. Das gilt insbesondere für die Werbung. Auch nach der DS-GVO ist dieser Umstand nicht anders zu beurteilen.

Seit dem 25. Mai 2018 ist Grundlage für die Beurteilung der Zulässigkeit von Werbung nach der DS-GVO, abgesehen von einer Einwilligung, eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Gemäß ErwGr 47 DS-GVO sind bei dieser Interessenabwägung die „vernünftigen Erwartungen der betroffenen Person, die auf

ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen.“ Werbende müssen die Informationspflichten nach den Art. 13, 14 DS-GVO einhalten. Von Werbung betroffene Personen haben ein jederzeitiges und umfassendes Widerspruchsrecht, auf das sie ausdrücklich hinzuweisen sind (Art. 21 Abs. 2 bis 4 DS-GVO). Für die E-Mail-Werbung bleibt abzuwarten, welche Regelungen die geplante neue E-Privacy-Verordnung (siehe Nr. 5.1) enthalten wird.

13.10 Wohnungswirtschaft

Bereits im XII. Tätigkeitsbericht (Nr. 14.13) hat der Landesbeauftragte darauf hingewiesen, dass er die Einhaltung der Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“ des Düsseldorfer Kreises vom 27. Januar 2014 anlassunabhängig überprüfen werde. Hintergrund dafür waren mehrere begründete Einzelbeschwerden von Mietinteressenten. Mittlerweile wurden mehr als 30 Unternehmen, die jeweils mehr als 3000 Wohnungen vermieten und über das ganze Land Sachsen-Anhalt verteilt sind, einer Überprüfung unterzogen:

In etlichen Vordrucken der Vermieter wurde nach unterschiedlichen personenbezogenen Daten der Mietinteressenten gefragt, deren Beantwortung aber als „freiwillig“ bezeichnet wurde. Dies stößt auf datenschutzrechtliche Bedenken, da eine Erhebung personenbezogener Daten nur zulässig ist, wenn Sie auf einer wirksamen Einwilligung beruht oder eine Rechtsvorschrift dies erlaubt. Eine Einwilligung ist nur dann wirksam, wenn sie freiwillig und informiert erfolgt. Freiwilligkeit liegt nur dann vor, wenn der Betroffene eine echte Wahl hat und sie zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm Nachteile entstehen. Dies ist im Verhältnis Vermieter / Mietinteressent regelmäßig nicht gegeben, da faktische Zwänge – das Interesse des Interessenten, eine bestimmte Wohnung zu erlangen – dazu veranlassen, die erbetenen Angaben zu tätigen. Die Einwilligung ist daher in aller Regel kein geeignetes Mittel, personenbezogene Daten über Mietinteressenten zu erheben. Dies gilt selbst dann, wenn die Wohnungsunternehmen über einen gewissen Leerstand verfügen. Die Verarbeitung personenbezogener Daten durch Vermieter ist daher nur zulässig, soweit eine Rechtsvorschrift dies gestattet. Als entsprechende Vorschriften kamen zum Zeitpunkt der Prüfung § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG (Vertragserfüllung oder Interessenabwägung) in Betracht.

Darüber hinaus wurden personenbezogene Daten erhoben, die für das Mietverhältnis im Normalfall nicht von Bedeutung sind. Dazu gehören z. B. allgemeine Fragen zu Haustieren. Das Halten von Kleintieren (z. B. Hamster, Zierfische) führt regelmäßig nicht zu Auswirkungen im Rahmen des Mietverhältnisses, darf daher nicht erfragt werden (BGH, Urteil vom 20. März 2013, Az. VIII ZR 168/12). Nicht relevant in diesem Zusammenhang ist auch die Frage nach dem Besitz von Musikinstrumenten, da diese auch entsprechend den mietvertraglichen Pflichten genutzt werden können. Unzulässig ist ebenfalls die Frage nach dem Grund der Wohnungssuche oder nach der Dauer der gegenwärtigen Beschäftigung.

Zudem sind vollständige Kopien von Ausweisdokumenten zum Identitätsnachweis regelmäßig unzulässig, weil sie Angaben enthalten, die für das Mietverhältnis bedeutungslos sind. Dies gilt insbesondere für den Personalausweis. Zwar ist dessen Kopie nach dem neuen Personalausweisgesetz nicht mehr generell ausgeschlossen (siehe dazu Nr. 13.5). Für ein zukünftiges Mietverhältnis sind jedoch viele Einzelan-

gaben aus dem Personalausweis belanglos (z. B. Augenfarbe, Körpergröße, Foto) und damit nicht zu erheben. Der Landesbeauftragte empfiehlt, den Personalausweis oder andere Ausweisdokumente zum Nachweis der Identität einzusehen und einen schriftlichen Vermerk über die Einsichtnahme zu fertigen.

Die Einholung von Bonitätsauskünften ist nicht schon beim ersten Besichtigungstermin zulässig, bei dem etliche Interessenten erklären, dass sie die Wohnung anmieten wollen. Sie ist rechtlich erst dann möglich, wenn sich der Vermieter für einen bestimmten Mieter entschieden hat und darf nur für diesen eingeholt werden.

Bescheinigungen, mithilfe derer Vermieter allgemeine Pflichtverletzungen eines Mietinteressenten beim Vorvermieter erfragen, sind grundsätzlich unzulässig. Sie können im Einzelfall nur zulässig sein, wenn lediglich solche Fragen gestellt werden, aus deren Beantwortung sich eine belastbare Prognose für das künftige Mietverhältnis ergibt (z. B. die Frage nach erheblichen Pflichtverletzungen, die eine außerordentliche Kündigung rechtfertigen und auch in Zukunft drohen könnten). Beachtet werden muss hier aber auch, dass es keine Verpflichtung des vorherigen Vermieters gibt, eine solche Bescheinigung auszustellen. Zudem sollte die Bescheinigung des Vorvermieters über den Mietinteressenten ausgehändigt werden.

Einige Vermieter stellten auf Ihren Homepages Online-Formulare bereit, in die Mietinteressenten etliche personenbezogene Daten eintragen konnten. Die Vermieter wurden darauf hingewiesen, dass diese Formulare zu verschlüsseln sind (vgl. Nr. 10.1.7). Die Nichtbeachtung dieses Hinweises führte zur Einleitung von Bußgeldverfahren.

Auch die zulässigen Löschfristen wurden häufig überschritten. Wenn ein Mietinteressent nicht erklärt, dass der Vermieter die Daten auch z. B. für zukünftig freiwerdenden Wohnraum nutzen darf, wären die Daten des Interessenten regelmäßig nach 6 Monaten zu löschen. Liegen besondere Gründe vor, könnten die Daten eines Mietinteressenten länger gespeichert werden. Wird z. B. der Mietinteressent wegen einer eingeholten Bonitätsauskunft abgelehnt, wäre die Speicherung für ein Jahr zulässig.

Viele der Unternehmen haben aufgrund der Prüfung und Beratung des Landesbeauftragten die Verarbeitung von Mietinteressentendaten angepasst.

Die Prüfung bei den Großvermietern hat gezeigt, dass es zu zahlreichen nicht zulässigen Verarbeitungen personenbezogener Daten von Mietinteressenten kam. Alle Vermieter sind verpflichtet, bei ihren Verarbeitungen personenbezogener Daten die DS-GVO und das BDSG 2018 anzuwenden. Hilfreich dazu ist eine aktualisierte Orientierungshilfe der DSK zu den Selbstauskünften der Mietinteressenten, die auf der Homepage des Landesbeauftragten verfügbar ist.

13.11 Anerkennung ausländischer Berufsqualifikationen

Aufgrund europarechtlicher Vorgaben war das Landesrecht zur Anerkennung ausländischer Berufsqualifikationen zu ändern. Unter anderen ging es um die Einführung eines Vorwarnmechanismus bei Untersagung und Einschränkung der Berufsausübung unter Nutzung des europäischen Binnenmarkt-Informationssystems (IMI) und die Eröffnung der Möglichkeit, Anerkennungsverfahren auch über den einheitlichen Ansprechpartner führen zu können. Bei der Erarbeitung des Entwurfs eines Zweiten

Gesetzes über die Anerkennung im Ausland erworbener Berufsqualifikationen im Land Sachsen-Anhalt wurde der Landesbeauftragte durch das Ministerium für Wissenschaft, Wirtschaft und Digitalisierung frühzeitig einbezogen. Neben redaktionellen Hinweisen konnte die Ausgestaltung der Umsetzung des Zitiergebotes (Art. 20 Abs. 1 Satz 2 Verf ST) in einem alle Artikel erfassenden gesonderten Artikel angeregt werden.

Regelungen zur Übermittlung von Daten an das Statistische Bundesamt und die Ämter der Länder wurden nicht mehr aufgenommen, da diese Regelungen im Hinblick auf die Vorschriften in § 15 Abs. 2 und 3 StatG-LSA überwiegend obsolet erschienen.

In Bezug auf die Ergänzung des Einheitlicher-Ansprechpartner-Gesetzes wurde in Frage gestellt, ob angesichts der Dokumentation (Speicherung) der Vorgänge bei den jeweils zuständigen Stellen die komplette Speicherung als Doppel beim einheitlichen Ansprechpartner erforderlich ist. Der Landesbeauftragte verwies auf die verfassungsrechtlich gebotene Datensparsamkeit. Die Dokumentation für den Nachweis im Verwaltungsverfahren sollte sich auf die eigene Aufgabe des einheitlichen Ansprechpartners beschränken und nicht die Aufgaben der zuständigen Stellen erfassen. Dieser Aspekt wurde zumindest in die Begründung aufgenommen. Der Anregung, die Dokumentation des einheitlichen Ansprechpartners von 5 Jahren auf 2 Jahre zu begrenzen, wurde gefolgt. Gleiches gilt für den Hinweis, dass der einheitliche Ansprechpartner dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung der Datensicherheit zu treffen hat.

Darüber hinaus wurde zu den umfänglichen Informationspflichten im Vorwarnmechanismus angemerkt, dass es Verfahrensalternativen gibt, die wesentlich datensparsamer sind. Aufgrund der Vorgaben aus Art. 56a der Richtlinie 2005/36/EG in Verbindung mit der EU-Durchführungsverordnung 2015/983 blieb insoweit aber kein Verbesserungsspielraum.

Zusätzlich wurde in organisatorischer Hinsicht die Notwendigkeit in Frage gestellt, Regelungen zur elektronischen Identifikation zu treffen, nämlich durch Verordnungen Diensteanbieter zu bestimmen, die Identifizierungskomponenten bereitstellen. Mit dem Beitritt des Landes Sachsen-Anhalt zu Dataport und der Überleitung des Landesrechenzentrums zu Dataport ab 1. Januar 2014 hat das Land jedoch bereits eine zentrale IT-Dienstleisterin.

Das Zweite Gesetz über die Anerkennung im Ausland erworbener Berufsqualifikationen im Land Sachsen-Anhalt vom 25. Februar 2016 ist am 4. März 2016 in Kraft getreten (GVBl. LSA 2016, S. 89).

13.12 Länderübergreifende Prüfungen von Übermittlungen in Drittstaaten

Die starke Vernetzung und Globalisierung von Geschäftsprozessen der Privatwirtschaft führt inzwischen in erheblichem Umfang zu Übermittlungen personenbezogener Daten in sog. Drittstaaten, d. h. in Staaten außerhalb der EU und des EWR. Dies betrifft nicht nur international tätige Großkonzerne, sondern auch kleinere und mittlere Unternehmen. Eine typische Fallgestaltung solcher Datenübermittlungen ist z. B. die Nutzung von Cloud-Computing-Anbietern für bestimmte Geschäftsprozesse. Erfahrungen aus den Beratungen der Aufsichtsbehörden zeigten, dass sich Unterneh-

men der Tatsache einer Datenübermittlung in Drittstaaten nicht immer hinreichend bewusst sind.

Die Übermittlung personenbezogener Daten in sog. Drittstaaten erfordert gegenüber „innereuropäischen“ Übermittlungen die Erfüllung zusätzlicher datenschutzrechtlicher Anforderungen (vgl. XII. Tätigkeitsbericht, Anlage 35). Durch die Verabschiedung des Privacy Shield (Nr. 3.2.1) war eine neue Situation eingetreten. Der Landesbeauftragte sah hierin – gemeinsam mit anderen deutschen Datenschutzaufsichtsbehörden – einen sinnvollen Zeitpunkt für eine koordinierte Prüfung des internationalen Datenverkehrs. An der Prüfungsaktion waren die Datenschutzaufsichtsbehörden aus Bayern, Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Sachsen-Anhalt innerhalb ihres jeweiligen Zuständigkeitsbereichs beteiligt.

In einem Fall wies der Landesbeauftragte darauf hin, dass Datenübermittlungen in die USA nicht mehr auf die Safe-Harbor-Entscheidung der Europäischen Kommission vom 26. Juli 2000 gestützt werden dürfen. Durch Urteil vom 6. Oktober 2015 hat der EuGH diese Kommissionsentscheidung für ungültig erklärt. Seit dem 1. August 2016 enthält das Privacy Shield Aussagen über den Schutz personenbezogener Daten, die aus einem Mitgliedstaat der Europäischen Union in die USA übertragen werden. Die Europäische Kommission hat mit Beschluss vom 12. Juli 2016 entschieden, dass das Privacy Shield ein angemessenes Schutzniveau gewährleistet (zu Details und Kritik am Privacy Shield s. Nr. 3.2.1).

Ein weiterer Fall gab dem Landesbeauftragten Anlass zu dem Hinweis, dass personenbezogene Daten von Bewerbern für ein Beschäftigungsverhältnis zwar in eng umgrenzten Fällen auf Grundlage von deren Einwilligungen in Länder ohne angemessenes Datenschutzniveau übermittelt werden durften (§ 4c Abs. 1 Satz 1 Nr. 1 BDSG). Allerdings musste die Einwilligung hierzu den Anforderungen des § 4a BDSG genügen und von den Bewerbern insbesondere freiwillig erteilt werden. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis hätten sich jedoch nicht dann freiwillig im Sinne von § 4a Abs. 1 BDSG entscheiden, wenn sie für den Fall der unterbliebenen Einwilligung Nachteile – wie z. B. ein vorzeitiges Ausscheiden aus dem Bewerbungsverfahren – befürchten mussten. In solchen Fällen stellte die Einwilligung somit keine taugliche Rechtsgrundlage für die Datenübermittlung in Länder ohne angemessenes Datenschutzniveau dar.

Die Einwilligung in die Übermittlung personenbezogener Daten in Länder ohne angemessenes Datenschutzniveau („Drittstaaten“) ist nunmehr nach der DS-GVO in Art. 49 Abs. 1 Satz 1 lit. a als Ausnahmetatbestand definiert. Demgemäß ist die Vorschrift eng auszulegen. Eine wirksame Einwilligung in die Datenübermittlung in einen Drittstaat setzt hier zunächst eine ausdrückliche Einwilligung in die Weitergabe personenbezogener Daten für den konkreten Fall voraus. Außerdem ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären. Diese Aufklärung muss sich vor allem auf das Fehlen eines angemessenen Datenschutzniveaus im Drittstaat und darauf beziehen, dass Betroffenenrechte dort ggf. nicht durchgesetzt werden können. Die betroffene Person ist auf die jederzeitige Widerrufbarkeit der Einwilligung hinzuweisen (Art. 7 Abs. 3 DS-GVO).

14 Videoüberwachung

14.1 Videoüberwachung durch nichtöffentliche Stellen

14.1.1 Allgemeines

Der Umfang der Videoüberwachung durch nichtöffentliche Stellen ist auch in diesem Berichtszeitraum weiter gestiegen (vgl. XII. Tätigkeitsbericht, Nrn. 15.2.1 ff.). Nach Schätzungen sind in Deutschland Hunderttausende Überwachungskameras im Betrieb, unter Umständen sogar Millionen. Allein in einem großen Einkaufszentrum in der Landeshauptstadt zählte der Landesbeauftragte mehrere Hundert. Besonders in den Innenstädten wird wohl nahezu jedermann täglich etliche Male von den Kameras erfasst und jede seiner Bewegungen im Erfassungsbereich gespeichert. Aber auch im nachbarschaftlichen Bereich hat der Einsatz von Videokameras zugenommen. Die vermehrte Überwachung mithilfe der Videotechnik führt zu mehr Beschwerden der abgelichteten Personen. Allein vom Kalenderjahr 2016 (49 Fälle) auf das Kalenderjahr 2017 (62 Fälle) erhöhte sich die Anzahl der Beschwerden beim Landesbeauftragten um ca. 26%. Auch wächst die Zahl der Anfragen zur Zulässigkeit von Videoüberwachungen nach der DS-GVO und dem BDSG 2018.

Die öffentliche Diskussion um die Videoüberwachung wird sehr kontrovers geführt. Aus Gründen der Gefahrenabwehr, Strafverfolgung und Geltendmachung von Schadensersatzansprüchen wird sie häufig befürwortet. Kritikern zufolge führt das maßlose Ausufern der Überwachung zu unverhältnismäßigen Eingriffen in die informationelle Selbstbestimmung. Forderungen nach einer generellen Meldepflicht für Überwachungskameras werden lauter.

Videotechnik ist preisgünstig. Für weniger als 300 Euro kann im Versandhandel ein Set, bestehend aus mehreren Kameras mit Funkübertragung, einem 2 TB Festplattenspeicher und einem Touchscreen erworben werden. Die Technik genügt höchsten Ansprüchen. Die Aufnahmen sind hochauflösend und in Farbe. Auch eine gute Nachtsicht wird oft versprochen. Für eine Gesichtserkennung müssen nur wenige Euro mehr ausgeben werden.

Allzu selten wird von den Betreibern der Videoüberwachung berücksichtigt, dass der Datenschutz hohe Hürden für die Verarbeitung personenbezogener Daten mithilfe von Videotechnik setzt. Dies gilt insbesondere mit Blick auf die DS-GVO, die den derzeitigen hohen Schutzstandard aufrechterhält. Nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ist eine Verarbeitung personenbezogener Daten auch durch eine Videoüberwachung nur zulässig, sofern ein berechtigtes Interesse vorliegt und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Besonderen Schutz genießen auch hier Kinder. Die Verarbeitung biometrischer Daten mithilfe einer Gesichtserkennung zur eindeutigen Identifizierung natürlicher Personen ist grundsätzlich untersagt. Entgegen mancher Behauptungen gestattet die DS-GVO eine Videoüberwachung nur mit eindeutigem Zwecknachweis, auch wenn diese nicht systematisch und umfangreich stattfindet. Nach Art. 5 Abs. 2 DS-GVO muss der Verantwortliche (der Betreiber der Videoüberwachung) die Einhaltung nachweisen. Hinzu kommt, dass – vorausgesetzt, die materielle Zulässigkeit ist gegeben – in formeller Hinsicht weitere Maßgaben erfüllt werden müssen:

- Aus Art. 13 DS-GVO ergibt sich, dass jeder Betreiber einer Videoüberwachung über die Identität des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten (wenn benannt), die Verarbeitungszwecke und die Rechtsgrundlage, das berechtigte Interesse, die Dauer der Speicherung und über den Zugang zu weiteren Pflichtinformationen informieren muss.

- Nach Art. 30 Abs. 1 DS-GVO ist ein Verzeichnis über die Videoüberwachung anzulegen, in dem unter anderem die Zwecke der Verarbeitung und die betroffenen Personen dokumentiert werden müssen.

- Führt die Videoüberwachung zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, ist eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchzuführen. Dies gilt insbesondere bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Eine Missachtung dieser Voraussetzungen kann zu aufsichtsbehördlichen Einschränkungen und Verboten der Überwachung sowie Bußgeldern führen. Weitere Einzelheiten zu den Voraussetzungen der Videoüberwachung nach der DS-GVO sind dem Kurzpapier Nr. 15 der DSK zu entnehmen. Im Übrigen werden die Orientierungshilfen (des Düsseldorfer Kreises) an die DS-GVO angepasst.

14.1.2 Videoüberwachungsverbesserungsgesetz

Im Mai 2017 trat das „Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen („Videoüberwachungsverbesserungsgesetz“, BGBl. I S. 968) in Kraft. Ziel des Gesetzes war es, die Sicherheit bei öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, sowie Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs zu erhöhen. Damit sollten unter anderem Anschläge wie in Ansbach und München im Sommer 2016 verhindert werden (BT-Drs. 18/10941). Der neu angefügte Satz 2 zu § 6b Abs. 1 BDSG sah bei der Videoüberwachung in den oben genannten Bereichen den Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein „besonders wichtiges Interesse“ an und enthielt damit eine normative Gewichtungsvorgabe.

§ 6b BDSG sah zuvor bereits vor, dass eine Videoüberwachung öffentlich zugänglicher Räume zur Wahrnehmung des Hausrechts oder im Rahmen einer Interessenabwägung zwischen den Rechten Betroffener und den Betreiberinteressen zulässig sein kann. Auch zur Beweissicherung konnte die Videoüberwachung damit eingesetzt und die Daten nach § 6b Abs. 3 Satz 3 BDSG an die zuständigen Ermittlungs- und Strafverfolgungsbehörden übermittelt werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich war.

Der Gesetzentwurf der Bundesregierung wurde von den Datenschutzbehörden des Bundes und der Länder abgelehnt (s. Entschließung in **Anlage 10**), da die Videoüberwachung durch private Betreiber nicht geeignet erscheint, das Ziel dieser gesetzlichen Regelung zu erreichen. Gemäß § 1 SOG LSA und § 3 BPolG obliegt die Aufgabe der Gefahrenabwehr den Sicherheitsbehörden und der Polizei und es ist

eben nicht Aufgabe privater Stellen, die Sicherheit der Bevölkerung zu gewährleisten. Auch die Frage, ob eine Gefahrenlage vorliegt, die eine Videoüberwachung rechtfertigt, kann wohl kaum von den nichtöffentlichen Stellen beurteilt werden. Hinzu kommt, dass Anschläge von Terroristen und Straftätern erfahrungsgemäß nicht durch eine Videoüberwachung verhindert werden können bzw. sie sich bei ihren Taten auch nicht durch Videokameras abschrecken lassen werden. Fraglich ist zudem, ob die Betreiber von Videoüberwachungsanlagen bei Gefahren unmittelbar eingreifen und Gefahrenabwehrmaßnahmen einleiten können.

Das am 25. Mai 2018 in Kraft getretene BDSG 2018 (vgl. Art. 1 DSAnpUG-EU) enthält in § 4 die identische Regelung aus dem Videoüberwachungsverbesserungsgesetz. Eine Videoüberwachung ist generell nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu beurteilen. Da die DS-GVO hier keinen weiteren Regelungsspielraum vorsieht, ist nach Ansicht des Landesbeauftragten die in § 4 BDSG 2018 übernommene Regelung des Videoüberwachungsverbesserungsgesetzes aufgrund des Anwendungsvorrangs der DS-GVO einschränkend auszulegen.

14.1.3 Videoüberwachung durch Privatpersonen

Wie in den vergangenen Berichtszeiträumen hat der Landesbeauftragte auch in diesem wieder eine Vielzahl an Beschwerden hinsichtlich des Einsatzes von optisch-elektronischen Einrichtungen (Videokameras) durch Privatpersonen erhalten.

Einige verantwortliche Stellen teilten auf eine erste Anfrage seitens des Landesbeauftragten mit, dass es sich bei den angebrachten Einrichtungen um Kameraattrappen handelt. Kameraattrappen wirken auf potenzielle Täter abschreckend, ohne dass es einer tatsächlichen Datenverarbeitung bedarf. Da mit Kameraattrappen keine personenbezogenen Daten erhoben oder verarbeitet werden, war der Anwendungsbereich des BDSG sowie nach der seit dem 25. Mai 2018 geltenden DS-GVO (inkl. BDSG 2018) nicht eröffnet, sodass diese Einrichtungen nicht der Kontrolle des Landesbeauftragten unterlagen. Allerdings sollten Privatpersonen auch hierbei beachten, dass betroffene Personen in der Regel Kameraattrappen von aktiven Kameras nicht unterscheiden können und sich demzufolge auch von Attrappen beeinträchtigt fühlen sowie zivilrechtlich zur Wehr setzen könnten. – Auch im engen Bereich der Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten findet das Datenschutzrecht keine Anwendung.

Sofern es sich um funktionsfähige, aktive Videokameras handelt, bestimmte sich die Zulässigkeit bei der Beobachtung öffentlich zugänglicher Räume nach § 6b BDSG, bei der Videoüberwachung nichtöffentlich zugänglicher Bereiche nach § 28 BDSG. Hier wird auf die Ausführungen, die der Landesbeauftragte in seinem XI. (Nr. 4.17.2) und XII. (Nr. 15.2.2) Tätigkeitsbericht dargestellt hat, verwiesen.

Wenn der Landesbeauftragte konkrete Anhaltspunkte für datenschutzrechtliche Verstöße erkennt, geht er den Beschwerden nach und wendet sich an die verantwortlichen Stellen, um entsprechende Auskünfte hinsichtlich der konkret durchgeführten Videoüberwachung einzuholen. Da einige verantwortliche Stellen zunächst keine Auskunft erteilten, musste der Landesbeauftragte in etlichen Fällen mittlerweile be-

standskräftige Verpflichtungsbescheide fertigen, mitunter mit Zwangsgeldandrohung bzw. -festsetzung.

Darüber hinaus hat der Landesbeauftragte die verantwortlichen Stellen beraten und unterstützt und darauf hingewirkt, dass datenschutzrechtliche Verstöße beseitigt wurden (vgl. § 38 Abs. 5 BDSG). So wurden im Berichtszeitraum in vielen der geprüften Fälle die Kameraeinstellungen bemängelt. Denn oftmals werden weite Teile des öffentlich zugänglichen Bereiches mit von den Kameras erfasst, was nur sehr begrenzt bei Vorliegen eines gewichtigen berechtigten Interesses zulässig ist. Dazu kamen vermehrt Verstöße bei der Speicherfrist. Der Landesbeauftragte konnte aber im Berichtszeitraum gegenüber vielen privaten verantwortlichen Stellen eine datenschutzkonforme Videoüberwachung erwirken – in nahezu allen Fällen auch ohne den Erlass einer Anordnung nach § 38 Abs. 5 BDSG.

Auch für Privatpersonen gilt seit dem 25. Mai 2018 die DS-GVO. Eine Datenverarbeitung mittels Videoüberwachung ist nunmehr nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu beurteilen. Werden öffentlich zugängliche Bereiche von der Videoüberwachung erfasst, ist stets davon auszugehen, dass die DS-GVO anzuwenden ist. Für Privatpersonen ergeben sich dann z. B. Neuerungen aus den Transparenzpflichten. Bei der Erhebung personenbezogener Daten sind den von der Videoüberwachung betroffenen Personen nach Art. 13 DS-GVO mehr Informationen zur Verfügung zu stellen. Hierbei ist der Informationskatalog des Art. 13 Abs. 1 und 2 DS-GVO zu beachten. Verstöße gegen die Transparenzpflichten stellen zudem einen Bußgeldtatbestand nach Art. 83 Abs. 5 DS-GVO dar. Dies gilt entsprechend für die Missachtung der Pflichten aus Art. 30 und Art. 35 DS-GVO.

14.1.4 Gesichtserkennungssoftware in Spielbanken

Bereits im XII. Tätigkeitsbericht (Nr. 15.2.5) schilderte der Landesbeauftragte seine Beratungstätigkeit im Hinblick auf eine im Jahr 2014 in Sachsen-Anhalt eröffnete Spielbank, insbesondere im Hinblick auf die dort installierte Videoüberwachungsanlage. Im Jahr 2016 wurde durch dieselbe Betreibergesellschaft in Sachsen-Anhalt eine zweite Spielbank eröffnet. Die Konzeption der dortigen Videoüberwachungsanlage konnte vor dem Hintergrund der Erfahrungen aus den Jahren 2014 und 2015 sehr effizient begleitet werden. Wieder im Dialog mit dem für Spielbankaufsicht zuständigen Ministerium für Inneres und Sport des Landes Sachsen-Anhalt wurden die Maßstäbe, die bereits im Verfahren 2014/2015 angelegt wurden, herangezogen und in nur einem Vor-Ort-Termin nach § 38 Abs. 4 BDSG eine datenschutzgerechte Lösung gefunden.

Die Betreibergesellschaft der Spielbanken wandte sich mit einer weiteren Beratungsanfrage an den Landesbeauftragten. Beabsichtigt war, die Einlasskontrolle in den Spielbanken durch eine biometrische Gesichtserkennungs-Software zu unterstützen, das sog. Face-Check-System. Kunden, die die Spielbanken mindestens zum dritten Mal aufsuchten, sollte angeboten werden, in Zukunft eine erleichterte und schnellere Einlasskontrolle durch biometrische Gesichtserkennung in Anspruch zu nehmen. Dazu werden von ihren Gesichtsfotos Templates erstellt, die mit Templates von gesperrten Spielern, die aus der staatlichen Spieler-Sperrdatenbank stammen, automatisiert verglichen werden. Ergibt der Vergleich keine Übereinstimmung, kann der

Kunde die Spielbank sofort betreten. Damit sollten Wartezeiten an den Eingängen vermieden und die Erkennungsrate von Spielersperren erhöht werden. Denn zuweilen käme es vor, dass durch Fehler bei der manuellen Eingabe der persönlichen Daten der Gäste ein eigentlich gesperrter Spieler Einlass erhalte.

In die Sperrdatei eingetragen werden Personen, die dies beantragen (Selbstsperre) oder die spielsuchtgefährdet oder überschuldet sind oder zu sein scheinen, die ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre). In die Sperrdatei wird der Grund der Sperre eingetragen (§ 5 Abs. 1 SpielbG LSA, § 14 GlüG LSA, § 8 Abs. 1 und 2 GlüStV). Der automatisierte Abgleich mit der Sperrdatei mittels eines biometrischen Datums erhöht die Intensität der Datenverarbeitung.

Bei der Prüfung der Zulässigkeit des Face-Check-Systems ist zu beachten, dass es sich bei einem Abgleich mit der Sperrdatei häufig um die Nutzung von Gesundheitsdaten handelt, denn die Sperrdatei dient dem Schutz der Spieler und zur Bekämpfung einer Krankheit – der Glücksspielsucht. Gesundheitsdaten gehören nach Art. 9 Abs. 1 DS-GVO zu den besonderen Kategorien personenbezogener Daten, deren Verarbeitung nur in den in Art. 9 Abs. 2 DS-GVO benannten Fällen zulässig ist. Darüber hinaus enthalten die Templates, die von Besuchern erstellt werden, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, die nunmehr ebenfalls zu den besonderen Kategorien personenbezogener Daten zählen.

Die Planungen der verantwortlichen Stelle für die Einführung der Gesichtserkennungs-Software sind noch nicht abgeschlossen. Seit dem 25. Mai 2018 sind nunmehr die Voraussetzungen der DS-GVO zu beachten. Nach Art. 9 Abs. 1 DS-GVO gehören auch biometrische Daten zu den besonderen Kategorien personenbezogener Daten, wenn sie der eindeutigen Identifizierung einer natürlichen Person dienen. Deren Verarbeitung ist dann nur zulässig, wenn die in Art. 9 Abs. 2 DS-GVO benannten Voraussetzungen erfüllt sind. Auch nach der DS-GVO kann damit bei dem hier vorliegenden Zweck die Datenverarbeitung nur auf eine wirksame Einwilligung gestützt werden. Zudem sollte vorab die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung geprüft werden, weil hier mehrere Datensätze miteinander automatisiert abgeglichen werden sollen, sich aus der Nutzung mehrerer besonderer Kategorien personenbezogener Daten eine besondere Schutzwürdigkeit ergibt und eine neue Technologie genutzt werden soll.

14.1.5 Videoüberwachung gegenüber Beschäftigten

Beim Landesbeauftragten gingen auch im aktuellen Berichtzeitraum einige Beschwerden ein, wonach Unternehmen Videokameras betreiben, die insbesondere auch die Beschäftigten aufnehmen. Vermehrt wurde in den angeforderten Stellungnahmen dargelegt, dass die Beschäftigten mit der Videoüberwachung einverstanden seien.

Grundsätzlich hat § 4 Abs. 1 BDSG vorgesehen, dass eine wirksame Einwilligung eine gesetzliche Erlaubnisnorm ersetzen kann. Nach § 4a Abs. 1 Satz 1 BDSG war eine Einwilligung jedoch nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruhte. Die Einwilligungen müssen der Verarbeitung personenbezogener Daten vorausgegangen sein. Die Freiwilligkeit setzte voraus, dass Betroffene ein echtes Wahlrecht hatten, d. h. die Einwilligungen auch folgenlos verweigern und ggf.

widerrufen konnten, ohne dass ihnen hieraus Nachteile entstanden. Die Betroffenen durften sich nicht in einer Situation (z. B. einem Abhängigkeitsverhältnis oder deutlichen Verhandlungsungleichgewicht) befinden, die sie faktisch dazu zwang, sich mit dem Zugriff auf ihre Daten einverstanden zu erklären.

Dass sich abhängig Beschäftigte auch im bestehenden Arbeitsverhältnis typischerweise in einer Situation struktureller Unterlegenheit befinden, ist in ständiger Rechtsprechung anerkannt. Zweifel an der Freiwilligkeit der Einwilligungserklärungen können sich zudem auch aus weiteren Umständen ergeben, z. B. aus einem Mangel an Ausweichmöglichkeiten. Es kann ferner ein Gruppenzwang vorliegen, wenn Einwilligungen auf Listen eingeholt werden, auf denen die Namen der Beschäftigten vorgedruckt sind. Wenn sich einzelne Beschäftigte nicht einverstanden erklären, würde dies für die anderen Beschäftigten sichtbar.

Weitere gesetzliche Voraussetzung war, dass die betroffenen Personen zum Zeitpunkt der Erteilung der Einwilligung im Detail über den Umfang der Datenverarbeitung informiert sein mussten. Sie mussten die Tragweite der Datenverarbeitung abschätzen können, z. B. durch Einblick in Referenzaufnahmen und das Verfahrensverzeichnis oder anderweitiges Informationsmaterial. Daneben war zu berücksichtigen, dass die Einwilligung der Beschäftigten die Videoüberwachung in keiner Weise rechtfertigen konnte, wenn auch Kunden, Lieferanten oder Passanten in den Erfassungsbereich geraten, die nicht eingewilligt hatten. Aufgrund der hohen Anforderungen an eine Einwilligung bei einer Videoüberwachung von Dauerarbeitsplätzen hat der Landesbeauftragte davon abgeraten, diese Lösung in Erwägung zu ziehen und empfohlen, den gesetzlich zulässigen Rahmen nicht zu überschreiten.

Im Rahmen der Prüfung der Beschwerden konnte der Landesbeauftragte bei den verantwortlichen Stellen auf datenschutzfreundliche Ausgestaltungen der Videoüberwachungen hinwirken bzw. bestätigen. In einem Fall beispielsweise befanden sich in dem Unternehmen nicht aktivierte bzw. nicht angeschlossene Videokameras, in zwei weiteren Fällen wurde die Videoüberwachung nur außerhalb der Geschäfts- bzw. Öffnungszeiten eingesetzt, um im Hinblick auf Einbrüche, Diebstahl und unbefugtes Betreten des Firmengeländes potenzielle Täter abzuschrecken und um im Rahmen der Strafverfolgung Beweise zu sichern. Da allerdings auch inaktive Kameras einen Überwachungsdruck auslösen und die Beschäftigten sich hiervon beeinträchtigt fühlen könnten, regte der Landesbeauftragte in diesen Fällen an, die Beschäftigten darüber zu informieren, dass die Kameras während der Geschäftszeiten deaktiviert sind. In einem anderen Fall stellte der Inhaber eines Betriebes sogar seine Videoüberwachung in Gänze ein und demontierte die Kameras, nachdem der Landesbeauftragte aufgezeigt hatte, dass die Videoüberwachung, so wie sie ausgestaltet war, nicht der Zweckerreichung dienen konnte.

Im Beschäftigtendatenschutz hat der deutsche Gesetzgeber vom Regelungsspielraum des Art. 88 DS-GVO Gebrauch gemacht und die Verarbeitung personenbezogener Daten von Beschäftigten in § 26 BDSG 2018 geregelt. Im Wesentlichen wurde die bisher geltende deutsche Rechtslage beibehalten. Im Bereich der Videoüberwachung von Beschäftigten richtet sich die Zulässigkeit i. d. R. nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Daneben ist die Datenverarbeitung grundsätzlich auch aufgrund einer Einwilligung gemäß Art. 6 Abs. 1 Satz 1 lit. a, Art. 7 DS-GVO möglich, soweit sie freiwillig erfolgt. Bei der Videoüberwa-

chung von Beschäftigten kommt eine Einwilligung nur in seltenen Fällen in Betracht, da i. d. R. infolge des Abhängigkeitsverhältnisses ein klares Ungleichgewicht besteht und es in Anbetracht aller Umstände unwahrscheinlich sein wird, dass die Einwilligung freiwillig gegeben werden würde (vgl. ErwGr 43 DS-GVO).

14.1.6 Videoüberwachung in öffentlichen Verkehrsmitteln

Dass trotz des Vorliegens der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ datenschutzrechtlicher Beratungs- und Klärungsbedarf bei Verkehrsunternehmen in Bezug auf die Videoüberwachung besteht, hatte der Landesbeauftragte in Nr. 15.2.8 seines XII. Tätigkeitsberichts bereits berichtet. Der dort genannte Fall, in dem Betriebsrat und Beschäftigte den schwerwiegenden Vorwurf erhoben, ihr Verkehrsunternehmen missbrauche die Videoüberwachung in den Fahrzeugen zweckfremd zur Verhaltens- und Leistungskontrolle des Fahrpersonals, konnte weitgehend abgeschlossen werden, wobei jedoch umfangreiche Kontrollen und Beratungen voraus gingen.

Im Ergebnis wurden dem Verkehrsunternehmen die folgenden Hinweise zur Optimierung der Videoüberwachung in seinen Fahrzeugen gegeben:

- Die Leistungs- und Verhaltenskontrolle der Mitarbeiter mittels Videoüberwachungsanlagen ist nach der für das Unternehmen geltenden Betriebsvereinbarung untersagt. Das gilt auch, wenn im Rahmen der Auswertung von Aufnahmen zu anderen begründeten Zwecken solche Daten über das Verhalten oder die Leistung der Beschäftigten als Nebenprodukt mit anfallen. Dabei erkannte Arbeitspflichtverletzungen dürfen keine arbeitsrechtlichen Maßnahmen, zu denen nach der herrschenden Meinung auch Ermahnungen und Belehrungen zu zählen sind, für die entsprechenden Mitarbeiter nach sich ziehen.

- Bei den Auswertungen der Videoüberwachungsaufnahmen ist gemäß Betriebsvereinbarung der Betriebsrat zu beteiligen, wenn Mitarbeiter des Unternehmens betroffen sind. Das war in mehreren Fällen tatsächlich unterblieben. Bei der Kontrolle wies der Landesbeauftragte darauf hin, dass die Nichtbeteiligung des Betriebsrates kein Mittel zur Gewährleistung von Datensparsamkeit darstellt. Der Betriebsrat ist bei der Auswertung der Videoaufnahmen kein Störfaktor, sondern soll u. a. bewirken, dass der Datenschutz und die Interessen der Belegschaft gewahrt bleiben. Seine Beteiligung ist schon deshalb wichtig, weil durch die Auswertung der Videoaufnahmen mitunter Verhaltensweisen von Mitarbeitern abgelichtet werden, die nicht Anlass zur Auswertung gegeben haben. So lassen die Videoaufnahmen oft erkennen, wie der Fahrer die Straßenbahn führt (z. B. Kurvengeschwindigkeit, Bremsverzögerung), ob er pflichtgemäß Überprüfungen der Straßenbahn an der Endhaltestelle vorgenommen hat oder wie er im Notfall Hilfe leistete. Eine Auswertung derartiger Erkenntnisse wäre zweckwidrig und damit nicht zulässig.

- Im Interesse einer lückenlosen Nachprüfbarkeit von Auswertungen der Videoaufnahmen durch Aufsichtsbehörde und Betriebsrat hat der Landesbeauftragte empfohlen, mehr Wert auf eine gründliche und fehlerfreie Protokollierung zu legen. Zur Dokumentation des Vier-Augen-Prinzips sollten Unterschriften der beiden auswertenden Personen im Protokollformular vorgesehen werden.

- In der Betriebsvereinbarung und der Betriebsleiteranweisung zur Videoüberwachung nimmt zwar die Angabe von Gründen für den Betrieb der Videoüberwachung breiten Raum ein. Dem Unternehmen wurde jedoch empfohlen, auch die Gründe, die eine Auswertung der Videoüberwachungsaufnahmen rechtfertigten, in die Protokolle aufzunehmen. Folgende Gründe für eine Auswertung der Videoüberwachungsaufnahmen wären vorstellbar: Beweissicherung bei tätlichen Übergriffen, Verursacherermittlung bei Sachbeschädigungen und Vandalismus, Aufklärung von Diebstählen und Täterermittlungen bei Straftaten außerhalb des Fahrzeuges.

- Um zu vermeiden, dass in betriebsbereiten Fahrzeugen bei Werkstattaufenthalten die Beschäftigten, z. B. Monteure oder das Reinigungspersonal, von der Videoanlage mit überwacht werden, muss eine Lösung gefunden werden, die Videoüberwachung erst zu aktivieren, wenn sich das Fahrzeug im Liniendienst auf der Strecke befindet.

14.1.7 Videoüberwachung an Tankstellen

Auch bei Tankstellen sind Videokameras inzwischen weit verbreitet, da die Betreiber oft mit einer hohen Gefahr im Hinblick auf z. B. Diebstähle und Raubstraftaten oder Tankbetrügereien rechnen. Stets muss die Videoüberwachung des öffentlich zugänglichen Raumes, wozu u. a. die Bereiche, in denen sich die Tanksäulen befinden oder zu denen auch der Verkaufsraum zählt, auf das für den Zweck erforderliche Maß beschränkt werden. Dazu gehört insbesondere die Begrenzung der Überwachung auf gefährdete räumliche Bereiche, die Hinweispflicht sowie die Pflicht, die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Zweckerreichung nicht mehr erforderlich sind.

Sofern auch die Beschäftigten von der Videoüberwachung betroffen sind, ist darüber hinaus ein besonderes Augenmerk auf den Beschäftigtendatenschutz (§ 32 BDSG bzw. § 26 BDSG 2018) zu legen. Die Videoüberwachung in Bereichen, in denen sich die Beschäftigten größten Teils während der Arbeitszeit aufhalten, ist oft problematisch, da sie sich der Überwachung aufgrund arbeitsvertraglicher Verpflichtungen häufig nicht entziehen können. In Tankstellen handelt es sich dabei z. B. um Kassenarbeitsplätze, d. h. die Bereiche hinter dem Kassentresen, Büro- oder Lagerräume. Eine Videoüberwachung zur Verhaltens- und Leistungskontrolle ist grundsätzlich unzulässig, ebenso wie die Überwachung von Umkleide- und Toilettenräumen sowie Pausenbereichen, die die Beschäftigten zur Erholung, Entspannung und Kommunikation nutzen.

Im Berichtszeitraum hat der Landesbeauftragte aufgrund eingegangener Beschwerden Videoüberwachungsanlagen in Tankstellen geprüft. Er hat darauf hingewirkt, dass die Tankstellenbetreiber datenschutzfreundliche Ausrichtungen bei den Kameraeinstellungen vorgenommen haben, sodass u. a. keine Kassenarbeitsplätze mehr im Erfassungsbereich sind oder diese durch Privatzonenmarkierungen ausgeblendet werden. Zudem konnte in den geprüften Fällen erreicht werden, dass die Speicherfrist entsprechend auf 48 Stunden reduziert wurde.

In einem Fall war die Datensicherheit bei der Übertragung an den Firmenhauptsitz (Fernzugriff) nicht sichergestellt, da keine Verschlüsselung erfolgte. Aufgrund des

Hinweises des Landesbeauftragten wurde die entsprechende Übermittlung eingestellt.

In einer weiteren Beschwerde wurde der Landesbeauftragte zudem darauf aufmerksam gemacht, dass in einer Tankstelle neben Video- auch Tonaufnahmen gefertigt werden. Das unbefugte Aufnehmen des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger ist im Falle eines Strafantrags gemäß § 201 StGB strafbar. Die Funktion für die Tonaufzeichnung wurde vom Tankstellenbetreiber deaktiviert und die gefertigten Tonaufnahmen gelöscht.

In Einzelfällen kann bei Videoüberwachungen auf größeren Tankstellenanlagen, Rast- und Autohöfen eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO erforderlich werden.

14.1.8 Videoüberwachung in Bäckereien

Aufgrund einiger begründeter Beschwerden und Hinweise aus der Zusammenarbeit mit den Landesbeauftragten anderer Bundesländer hatte sich der Landesbeauftragte entschlossen, eine anlassunabhängige Überprüfung bei Bäckereien mit größerem Filialnetz und Sitz in Sachsen-Anhalt durchzuführen.

Im Ergebnis war festzustellen, dass in fünf der zwölf geprüften Bäckereiketten keine aktive Videoüberwachung betrieben wurde. Dass demnach viele Unternehmen unter vergleichbaren Bedingungen eine Videoüberwachung nicht als erforderlich einschätzten, bestätigte die vorherige Annahme, dass keine abstrakte Gefahrenlage in Bäckereien und Bäckereifilialen vorliegt, die eine Videoüberwachung per se rechtfertigt.

In zwei Unternehmen fand eine Videoüberwachung an den Produktionsstätten statt. Die Unternehmen schilderten hierfür eine konkrete Gefahrenlage und gaben als berechtigte Interessen die Sicherung der Grundstücke und Gebäude gegen unbefugten Zutritt sowie die Verhinderung und ggf. Aufklärung wiederholter (Einbruch-) Diebstähle und Sachbeschädigungen an. Von den Videokameras erfasst wurden die Zufahrts- und Eingangsbereiche, aber auch zum Teil Vorbereitungsräume und eine Backstube. Besonders die letztgenannten Bereiche waren Gegenstand der Erörterungen. Nach der ständigen Rechtsprechung des Bundesarbeitsgerichtes ist bei der Überwachung von Beschäftigten ein besonders strenger Maßstab anzusetzen. Einer dauerhaften Mitarbeiterüberwachung müssen äußerst gewichtige berechtigte Interessen des Arbeitgebers gegenüberstehen. Eine Videoüberwachung zur Verhaltens- und Leistungskontrolle ist grundsätzlich unzulässig.

Bei einer Bäckereikette wurden in etlichen Filialen weite Bereiche hinter den jeweiligen Tresen – und damit die Arbeitsplätze der Beschäftigten – von der Videoüberwachung erfasst. Dies stellt wegen der dauernden Überwachung einen besonders intensiven Eingriff in die informationelle Selbstbestimmung dar. Die verantwortliche Stelle begründete die Überwachung mit von den Beschäftigten listenmäßig unterschriebenen Einwilligungserklärungen. Dies war nicht akzeptabel, da die Einwilligung hier keine Wirksamkeit entfalten konnte (siehe zur näheren Begründung Nr. 14.1.6). Auf den dringenden Rat des Landesbeauftragten wurde die Videoüberwachung auf eine gesetzliche Erlaubnisvorschrift gestützt und wesentlich beschränkt. Dies führte dazu, dass der Erfassungsbereich auf die Auslagen und die Aktivierung der Kameras

auf wenige Minuten pro Tag begrenzt sowie jeweils den Beschäftigten angekündigt wird.

Einige Unternehmen stellten infolge der aufsichtsbehördlichen Hinweise sicher, dass die eigentlichen Arbeitsplätze von der Videoüberwachung nicht mehr erfasst werden. Im Übrigen überwogen die schutzwürdigen Interessen der Betroffenen nicht, wenn sich Personen in den Erfassungsbereichen der wenigen Videokameras allenfalls kurzfristig aufhalten (vgl. §§ 6b und 28 Abs. 1 Satz 1 Nr. 2 BDSG). In diesen Fällen waren Hinweise der Aufsichtsbehörde bezüglich der notwendigen Beschilderung, der Speicherfrist von maximal 48 Stunden, zu angemessenen Maßnahmen der Datensicherheit sowie zu dem Erfordernis, ein Verfahrensverzeichnis zu führen, ausreichend, aber auch notwendig, um datenschutzgerechte Zustände zu gewährleisten.

Des Weiteren hatten sechs der geprüften Unternehmen Videokameras auch oder nur in den Verkaufsräumen installiert. Da allerdings diese Videoüberwachung in der Regel mit einer dauerhaften und beinahe lückenlosen Überwachung der Arbeitsbereiche der Beschäftigten verbunden war, stand die Aufsichtsbehörde diesen Datenverarbeitungen ebenfalls sehr kritisch gegenüber. Auch durch die individuelle technische Ausgestaltung, z. B. teilweise mit mobilem Zugriff auf die Videoströme für Vorgesetzte und die Geschäftsführung, war eine sehr hohe Eingriffsintensität festzustellen. In den zum Teil sehr ausführlichen Beratungsgesprächen mit den Unternehmen standen mögliche mildere Mittel und der Grundsatz der Datensparsamkeit (räumliche und zeitliche Einschränkung) im Vordergrund. Dabei hat die Aufsichtsbehörde erläutert, dass in Verkaufsräumen mit Kundenverkehr beispielsweise Folgendes datenschutzrechtlich zulässig sein kann, wenn eine entsprechende Gefahrenlage bzw. Notwendigkeit belegt ist und die Videoüberwachung lediglich:

- außerhalb der Geschäftszeiten zur Dokumentation von Einbrüchen, Diebstahl und Vandalismus,

- gekoppelt an Notrufmechanismen, die die Videokameras (nur) bei Bedarf aktivieren, zur Beweissicherung bei Raubüberfällen und zum Schutz der Beschäftigten an Einzelarbeitsplätzen

- oder bei einem dokumentierten konkreten Straftatverdacht gegen Beschäftigte, wenn sie zeitlich und räumlich eng auf die Aufklärung dieses Verdachts ausgerichtet und insgesamt nicht unverhältnismäßig ist,

stattfindet.

Drei Unternehmen stellten die Videoüberwachung in den Filialen nach zum Teil sehr aufwändiger aufsichtsbehördlicher Beratung in Gänze ein. Ein Unternehmen hat die Videoüberwachung während der Geschäftszeiten deaktiviert. In einem Unternehmen konnte die Aufsichtsbehörde erreichen, dass die Videoüberwachung nur noch auf die Kassentableaus beschränkt und die weiteren vorhandenen Videokameras deaktiviert wurden.

14.1.9 Dashcam – Crashcam

Die Problematik im Hinblick auf den Einsatz sog. Dashcams hat der Landesbeauftragte auch schon in seinem XII. Tätigkeitsbericht (Nr. 15.2.7) dargestellt. Dabei tref-

fen unterschiedliche Interessen aufeinander: zum einen die Interessen des Fahrzeugführers, der mithilfe der Dashcam-Aufnahmen im Zivilprozess seine Unschuld beweisen möchte, und zum anderen das Datenschutzrecht bzw. die allgemeinen Persönlichkeitsrechte anderer (mitgefilmter) Verkehrsteilnehmer.

Schon mehrfach hatten die Gerichte in der Vergangenheit über die Verwertbarkeit von Dashcam-Aufnahmen im Zivilprozess – teils uneinheitlich – geurteilt. Nunmehr hat der BGH höchstrichterlich mit Urteil vom 15. Mai 2018 (Az.: VI ZR 233/17) hierüber entschieden.

Hintergrund dafür war ein Unfallvorgang, bei dem die Beteiligten darüber streiten, wer von beiden seinen Fahrstreifen verlassen und die Kollision herbeigeführt hat. Dies wurde von einer Dashcam aufgezeichnet. Das Amtsgericht hat diese Aufnahmen im Prozess nicht als Beweismittel verwertet. Das Landgericht hat die Berufung des Klägers hierzu zurückgewiesen, da die Aufzeichnung gegen datenschutzrechtliche Bestimmungen verstoße und zudem einem Beweisverwertungsverbot unterliege.

Der BGH führt in seiner Urteilsbegründung aus, dass eine permanente anlasslose Aufzeichnung des Geschehens auf und entlang der Fahrstrecke – wie sie im zu prüfenden Sachverhalt vorlag – nicht zur Wahrnehmung der Interessen des Dashcam-Betreibers erforderlich ist und somit auch nicht auf § 6b Abs. 1 und § 28 Abs. 1 BDSG gestützt werden konnte. Da auch keine Einwilligungen sämtlicher betroffener Personen vorlagen, war die Datenverarbeitung gemäß § 4 Abs. 1 BDSG nicht zulässig (vgl. hierzu Rdnr. 19 des Urteils). Zudem gebe es technische Möglichkeiten, um eine dauerhafte Aufzeichnung zu vermeiden, indem lediglich eine kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen erfolge (Rdnr. 25 des Urteils). Hierbei handelt es sich um eine sog. „Crashcam“, die nur im Falle eines Unfalls, einer Kollision oder bei abruptem Abbremsen das Unfallgeschehen in einem geringen Zeitfenster aufzeichnet. Eine Langzeitspeicherung entfällt, da die Speicherkarte ständig überschrieben wird.

Der BGH hält bei der Frage der Verwertbarkeit rechtswidrig gefertigter Videoaufnahmen eine Güterabwägung im Einzelfall für erforderlich und kommt in dem vorliegenden Fall zu dem Ergebnis, dass die Interessen des Dashcam-Betreibers gegenüber dem Eingriff in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung überwiegen, sodass die Videoaufzeichnung in dem vorliegenden Fall als Beweismittel im Zivilprozess verwertbar ist (vgl. Rdnr. 39 ff. des Urteils).

Der Landesbeauftragte weist darauf hin, dass unabhängig von der Verwertbarkeit im Zivilprozess die Aufsichtsbehörden bei einer unrechtmäßigen Datenverarbeitung Verbote aussprechen und empfindliche Bußgelder verhängen können, die ggf. den Vorteil aus dem Zivilprozess aufheben. Er rät daher dringend von einer permanenten anlasslosen Aufzeichnung des Straßenverkehrs mittels Dashcam ab.

Der Beschluss des Düsseldorfer Kreises vom 25. und 26. Februar 2016 zur „Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)“ wird derzeit aufgrund der seit dem 25. Mai 2018 geltenden DS-GVO (relevant dürfte hier Art. 6 Satz 1 lit. f sein) sowie unter Berücksichtigung der aktuellen Rechtsprechung des BGH überarbeitet. Der Landesbeauftragte wird das Ergebnis veröffentlichen.

14.1.10 Webcams – Veröffentlichung von Bildnissen im Internet

Welche datenschutzrechtlichen Fallstricke der wie auch immer motivierte Betrieb einer Webcam für die verantwortliche Stelle mit sich bringt und wie man mögliche Rechtsverstöße als Verantwortlicher umgehen könnte, darüber hatte der Landesbeauftragte in seinem XI. Tätigkeitsbericht (Nr. 4.17.7) und XII. Tätigkeitsbericht (Nr. 15.2.11) bereits berichtet. Er hält seine dargestellte Ansicht und seine Empfehlungen auch vor dem Hintergrund der ab dem 25. Mai 2018 anzuwendenden DS-GVO und des BDSG 2018 aufrecht.

Sollen mithilfe einer Webcam Aufnahmen von erkennbaren natürlichen Personen gespeichert und im Internet veröffentlicht werden, wird dies in Zukunft nur zulässig sein, wenn gemäß Art. 6 Abs. 1 lit. f DS-GVO die Interessen oder Grundrechte und Grundfreiheiten der abgebildeten Person nicht überwiegen. Denn die Einholung einer Einwilligung des jeweiligen Betroffenen ist praktisch ausgeschlossen.

Im Ergebnis wird es kaum einen Zweck zum Betreiben einer Webcam geben, der es rechtfertigt, etliche Personen für jedermann im Internet abrufbar abzulichten. Jede verantwortliche Stelle einer Webcam ist demnach gut beraten, Kamerastandort und Bildauflösung so auszuwählen, dass auf den veröffentlichten Aufnahmen weder Personen noch sie identifizierende Gegenstände, wie z. B. amtliche Kennzeichen von Fahrzeugen, erkennbar sind. Damit werden Erhebung und Verarbeitung personenbezogener Daten durch die Webcam von Anfang an vermieden.

Für Webcam-Aufnahmen und auch für die Veröffentlichung von Bildnissen im Internet enthält das Kunsturhebergesetz (KunstUrhG) ergänzende Regelungen, die auch fortbestehen, seitdem die DS-GVO anzuwenden ist. Das KunstUrhG stützt sich speziell bei der Verarbeitung zu Zwecken der Meinungsfreiheit auf Art. 85 Abs. 1 der DS-GVO, der den Mitgliedstaaten nationale Gestaltungsspielräume bei dem Ausgleich zwischen Datenschutz und der Meinungs- und Informationsfreiheit eröffnet. Es steht nicht im Widerspruch zur DS-GVO, sondern fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der DS-GVO ein (vgl. speziell zu journalistischen Zwecken gem. Art. 85 Abs. 2 den Beschluss des OLG Köln vom 18. Juni 2018, Az.: 15 W 27/18). Diesen bisher vom Bundesministerium des Innern, für Bau und Heimat vertretenen Standpunkt teilen die DSK und so auch der Landesbeauftragte. Wenn also auf Internet-Aufnahmen Personen z. B. nur als Beiwerk der Aufnahme erscheinen, sind solche Aufnahmen auch ohne Einwilligung der Betroffenen zulässig (§ 23 Abs. 1 Nr. 2 KunstUrhG). Bei weitergehenden Aufnahmen mit einzelnen Fotos etwa zu Werbezwecken wäre die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu prüfen.

14.1.11 Private „Öffentlichkeitsfahndung“ im Internet unzulässig

Bei der Veröffentlichung von Videoaufnahmen mit personenbezogenen Daten handelt es sich um eine Übermittlung und damit um die Verarbeitung der Daten (vgl. § 3 Abs. 4 Satz 1 und Satz 2 Nr. 3 BDSG). Die Veröffentlichung von Videoaufnahmen konnte gemäß § 6b Abs. 3 BDSG zulässig sein, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (auch gem. DS-GVO ist eine solche Abwägung erforderlich).

Im aktuellen Berichtszeitraum ist der Landesbeauftragte auf drei Gastronomiebetreiber aufmerksam geworden, die Bild- bzw. Videoaufnahmen in einem sozialen Netzwerk veröffentlichten. Dabei handelte es sich in zwei Fällen um Videoaufnahmen von vermeintlichen Straftätern, die bei einer Einbruchshandlung in den Gastronomiebetrieb gefilmt wurden. In einem weiteren Fall wurde das Bildnis einer Person veröffentlicht, die nach Angaben des Gastronomiebetreibers Sachbeschädigungen an dessen Eigentum vorgenommen haben soll. Die Gastronomiebetreiber beabsichtigten mit Hilfe der Veröffentlichung der Aufnahmen in einem sozialen Netzwerk die Identität der Täter zu ermitteln.

Dass Öffentlichkeitsfahndungen in sozialen Netzwerken durch die Polizei datenschutzrechtlich problematisch sind, stellte der Landesbeauftragte auch bereits in den Tätigkeitsberichten XI. (Nr. 5.6) und XII. (Nr. 6.3) fest. Es handelt sich dabei um einen besonders intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Auch Personen, die Straftaten begehen, haben dieses Grundrecht nicht verwirkt. Ein derartiger Grundrechtseingriff durch die Gastronomiebetreiber war nicht gerechtfertigt und die Datenverarbeitung gemäß § 4 Abs. 1 BDSG nicht zulässig.

Vielmehr haben Geschädigte die Möglichkeit, Strafanzeige zu erstatten und zur Wahrnehmung des Hausrechts bzw. zur Verfolgung der eigenen berechtigten Interessen den Ermittlungsbehörden Videoaufnahmen oder anderes Beweismaterial zu übergeben (vgl. § 6b Abs. 3 Satz 2 BDSG), denn die Strafverfolgung obliegt den Ermittlungsbehörden. Im Rahmen ihrer Zuständigkeit prüfen diese, ob eine Öffentlichkeitsfahndung unter den Voraussetzungen der §§ 131 Abs. 3, 131a Abs. 3, 131b und 131c StPO erforderlich ist und ob die aufgezeichneten Daten zur Ermittlung der Straftäter im Internet veröffentlicht werden können.

Im Ergebnis wies der Landesbeauftragte die drei Gastronomiebetreiber auf die datenschutzrechtliche Problematik von Öffentlichkeitsfahndungen hin. In zwei Fällen wurden daraufhin die Bild- bzw. Videoaufnahmen der Personen aus dem sozialen Netzwerk gelöscht. In dem dritten Fall kam der Gastronomiebetreiber den Hinweisen zunächst nicht nach, sodass der Landesbeauftragte eine Anordnung gemäß § 38 Abs. 5 Satz 1 BDSG erließ, in der der Gastronomiebetreiber aufgefordert wurde, die im Internet veröffentlichten Videoaufnahmen zu löschen. Letztlich kam der Verantwortliche der Anordnung nach, indem er die Videoaufnahmen nachweislich löschte.

14.1.12 Speicherung von Videoaufnahmen in einer Cloud

Mittlerweile werden auch Videoüberwachungsanlagen angeboten, die eine Speicherung der Aufnahmen in einer Cloud ermöglichen. Allerdings sind für die Rechtmäßigkeit einer Speicherung von personenbezogenen Daten in der Cloud hohe Voraussetzungen zu erfüllen. Ein vom Landesbeauftragten überprüftes Produkt erfüllte diese Voraussetzungen in mehrfacher Hinsicht nicht. Problematisch waren insbesondere folgende Aspekte:

- Für die Speicherung in der Cloud wäre ein Vertrag über eine Auftragsverarbeitung erforderlich, den die verantwortliche Stelle (ggf. auch der Privathaushalt) mit dem Betreiber der Cloud abschließen müsste. Dabei müssen alle in Art. 28 Abs. 3 DS-GVO genannten Festlegungen getroffen werden. Verantwortlich für den Abschluss des Vertrages ist der Betreiber der Videoüberwachung, nicht der Hersteller.

- Die personenbezogenen Daten, die mithilfe von Videokameras erhoben wurden, sind unverzüglich zu löschen, wenn sie zur Zweckerreichung nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Nach der Orientierungshilfe „Videoüberwachung durch nichtöffentliche Stellen des Düsseldorfer Kreises“ vom 19. Februar 2014 sind solche Aufnahmen grundsätzlich nach 48 Stunden zu löschen. In dem vom Landesbeauftragten geprüften Produkt war eine Speicherfrist von mindestens sieben Tagen vorgegeben, was nicht zulässig war.

- Sofern die Videoaufnahmen auf einem Server außerhalb der EU/des EWR in einem Land ohne angemessenem Datenschutzniveau gespeichert wären, müssten zusätzliche Garantien bestehen, die den Schutz des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte von Betroffenen gewährleisten. Beispiele für solche Garantien sind EU-Standardverträge, Individualverträge, verbindliche Unternehmensregelungen zum Datenschutz und – bei Datenspeicherung in den USA – das Privacy Shield (siehe Nr. 3.2.1).

- Sofern die Videoaufnahmen innerhalb der EU von einem in der EU ansässigen Unternehmen gespeichert werden, welches aber einem außereuropäischen Mutterkonzern angehört, müsste sichergestellt werden, dass der Mutterkonzern nicht auf die Aufnahmen zugreift. Ein derartiger Zugriff ist z. B. bei US-amerikanischen Mutterkonzernen derzeit nicht ausgeschlossen. Im Jahr 2013 hatte Microsoft – trotz Vorliegens eines US-amerikanischen Durchsuchungsbefehls – die Herausgabe von E-Mails eines Verdächtigen verweigert, da diese auf einem Server in Irland gespeichert waren. Zwar hat sich auf Antrag des US-Justizministeriums das höchste US-Gericht, der Supreme Court, damit befasst und das Verfahren eingestellt. Seit dem Frühjahr 2018 werden jedoch amerikanische Unternehmen verpflichtet, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt.

- Bei der Übertragung in die (europäische) Cloud müsste gemäß Art. 5 Abs. 1 lit. f und Art. 32 Abs. 2 DS-GVO sichergestellt sein, dass personenbezogene Daten während der elektronischen Übertragung und der Speicherdauer nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies lässt sich erreichen, wenn die Videodaten vor oder während der Übertragung in die Cloud sicher verschlüsselt werden. Der Cloud-Anbieter müsste außerdem gewährleisten, dass die auf seinen Servern gespeicherten Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Das vom Landesbeauftragten überprüfte Produkt erfüllte die rechtlichen Anforderungen nicht. Die verantwortliche Stelle setzte die Videoüberwachung nach entsprechenden Hinweisen aus.

14.2 Videoüberwachung an Schulen

Die Landesregierung hat im September 2017 in einer Antwort auf eine Kleine Anfrage im Landtag von Sachsen-Anhalt (LT-Drs. 7/1843) zum Umfang der Videoüberwachung an Schulen im Land Stellung genommen. Auf die eigene Verantwortung der Schulträger wurde hingewiesen. Die Erkenntnisse aus den Rückmeldungen einer

Umfrage ergaben, dass es Videobeobachtungen, vor allem aber Videoaufzeichnungen gab. Aufgenommen wird innerhalb und außerhalb der Schulgebäude. Als Zwecke wurden u. a. die Eindämmung von Vandalismus, der Schutz vor körperlichen Übergriffen, die Einbruchsprävention, die Eintrittskontrolle und der Schutz von Fahrradständern genannt. Die angegebenen Speicherfristen reichten von 52 Stunden bis zu 8 Monaten. Die pauschalen Angaben waren wohl der Art der Darstellung geschuldet.

Ein rechtsstaatlicher Umgang mit Videoüberwachung an einer Schule bedarf der Berücksichtigung umfänglicher rechtlicher Vorgaben. Speicherungen von Aufzeichnungen über mehrere Monate erscheinen von vornherein grob rechtswidrig. Die Einhaltung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit ist im Einzelfall zu prüfen und zu belegen. Einschränkungen einer ggf. möglichen Beobachtung bzw. Aufzeichnung betreffen z. B. den Aufnahmeausschnitt und die Aufnahmezeiten. Zu Möglichkeiten und Grenzen einer Videoüberwachung von Objekten öffentlicher Stellen enthält der XII. Tätigkeitsbericht des Landesbeauftragten unter Nr. 15.1.1 umfassende Erläuterungen.

Da auch aus der Beratungstätigkeit und Prüfungspraxis vor Ort der Eindruck gewonnen wurde, dass in Schulen die Rahmenbedingungen der Speicherung und Verwendung von Videoaufnahmen nicht immer hinreichend bewusst sind, ist geplant, die Schulträger gemeinsam mit dem Ministerium für Inneres und Sport durch Sensibilisierungen und Fortbildungen bei der datenschutzkonformen Nutzung von Videoüberwachungstechnik zu unterstützen. Zunächst ist an ein Informationspapier gedacht.

Videoüberwachungen an Schulen sind nur in ganz engen Grenzen im Rahmen der Erforderlichkeit und Verhältnismäßigkeit zulässig.

15 Verkehr

15.1 VEMAGS-Staatsvertrag – Neuer Entwurf

Bereits seit 2008 wird das Verfahren flächendeckend in allen Ländern genutzt und steht damit den Antragstellern von Groß- und Schwerlasttransporten bundesweit zur Verfügung. Mit der Überführung des Testbetriebs in den ständigen Regelbetrieb im Jahr 2012 besteht seither für dieses automatisierte Verfahren unter der Bezeichnung VEMAGS (Verfahrensmanagement für Großraum- und Schwertransporte) die nachdrückliche Forderung nach einer gesetzlichen Grundlage in Form eines Staatsvertrages.

Der Landesbeauftragte hat zuletzt in seinem XII. Tätigkeitsbericht (Nr. 16.2) über die datenschutzrechtlichen Mängel im damaligen VEMAGS-Staatsvertragsentwurf aus dem Jahr 2014 berichtet. Ein wesentlicher Mangel in diesem Staatsvertragsentwurf betraf das sog. „Rotationsprinzip“ für die datenschutzrechtlich verantwortliche Stelle. Die Projektleitung von VEMAGS als die verantwortliche Stelle wäre demnach jeweils zeitlich befristet einem Land als Vertragspartner übertragen worden.

Im Dezember 2017 erreichte den Landesbeauftragten vom Ministerium für Landesentwicklung und Verkehr (MLV) eine entsprechende Anfrage zu einem *neuen*

VEMAGS-Staatsvertragsentwurf (Stand: 10. November 2017). In diesem Zusammenhang wurde eine Ratifizierung dieses Staatsvertrages vor dem 25. Mai 2018 mit Hinblick auf die dann geltende DS-GVO in Frage gestellt. Mit Hinweis auf die DS-GVO wurde die Überprüfung dieses aktuellen VEMAGS-Staatsvertragsentwurfs angeregt.

Rechtliche Überlegungen des MLV gingen dahin, dass eventuell der Abschluss eines Staatsvertrages bei Geltung der DS-GVO, insbesondere unter Beachtung bzw. Auslegung des Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche), nicht mehr erforderlich sei. Stattdessen könnte eine *vertragliche* Vereinbarung gem. Art. 26 DS-GVO mit den beteiligten Landesbehörden in Frage kommen.

Diese Überlegungen teilt der Landesbeauftragte nicht. Der Art. 26 DS-GVO ist eine organisatorische Regelung zur klaren Zuweisung von Verantwortlichkeiten. Er ist damit keine Rechtsgrundlage bzw. kann eine Rechtsgrundlage nicht ersetzen. Es bleibt bei dem Erfordernis einer Ermächtigungsgrundlage für die jeweilige Datenverarbeitung. Die gemeinsame Verarbeitung aller Daten der beteiligten Landesbehörden muss bundes- oder landesrechtlich fundiert sein.

Die Position des MLV ist nicht näher bekannt; dies gilt allgemein für die Frage nach dem weiteren Umgang mit dem VEMAGS-Staatsvertragsentwurf.

15.2 Autonomes Fahren

Um den Datenschutz bei der weiteren Entwicklung von modernen Kraftfahrzeugen sicherzustellen, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bereits seit dem Jahr 2015 Gespräche mit Vertretern der deutschen Automobilindustrie aufgenommen. Im Ergebnis dieses intensiven Dialogs steht die „Gemeinsame Erklärung der Datenschutzbeauftragten von Bund und Ländern und des Verbandes der Automobilindustrie (VDA)“ vom 26. November 2015 zu den datenschutzrechtlichen Aspekten bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge. Im Februar 2018 wurde ein Mustertext für eine Herstellerinformation zur Datenverarbeitung veröffentlicht.

Das Angebot an technischen Assistenzsystemen in Kraftfahrzeugen, die den Fahrzeugführer im Fahrbetrieb unterstützen, hat sich gerade auch im zurückliegenden Berichtszeitraum kontinuierlich ausgeweitet. Der Landesbeauftragte informierte in seinem XII. Tätigkeitsbericht (Nr. 16.3) bereits über die Forschungstätigkeiten auf diesem Gebiet, bei dem die Assistenzsysteme mit dem Ziel weiterentwickelt werden, dass sich das Kraftfahrzeug der Zukunft autonom, ohne Steuerung durch den Menschen, sicher im Straßenverkehr fortbewegen kann. Des Weiteren steht das vernetzte Kraftfahrzeug im Fokus der Forschung und Entwicklung. Es soll in Zukunft mehr und mehr Kontakt mit seiner Umwelt, d. h. mit anderen Kraftfahrzeugen, aber auch mit der Verkehrsinfrastruktur aufnehmen und kommunizieren. Die Automobilindustrie strebt für das Jahr 2030 das *autonome Fahren*, d. h. das fahrerlose Fahren eines Kraftfahrzeuges an.

Die Automobilindustrie unterscheidet vier Ausbaustufen:

- 1. Stufe – *Assistiertes Fahren* (Unterstützung durch Assistenzsysteme wie z. B. Spurhalte- und Bremsassistent, Tempomat, Abstandswarner, Totwinkelüberwachung u. a.),
- 2. Stufe – *Teilautomatisiertes Fahren* (z. B. auf Autobahnen selbständige Steuerung des Kraftfahrzeugs; die Übernahme Steuerfunktion durch den Menschen muss aber jeder Zeit möglich sein),
- 3. Stufe – *Hochautomatisiertes Fahren* (nicht nur automatisiertes Steuern ist möglich, sondern das Kraftfahrzeug findet z. B. seine Fahrtziele allein. Ein Eingriff des Kraftfahrzeugführers ist nur noch im Notfall nötig),
- 4. Stufe – *Vollautomatisiertes Fahren* (in bestimmten Fahrsituationen wie z. B. Überholen, Spurwechsel, Bremsen, Einparken u. ä. ist der Fahrzeugführer überflüssig).

Gegenwärtig befindet man sich bei modernen Kraftfahrzeugen in der 1. und 2. Stufe. Die 3. Stufe, das hochautomatisierte Fahren, steht noch bevor, es wird aber bereits seitens der Automobilindustrie intensiv daran geforscht und experimentiert.

Diese zukünftige Entwicklung zum hoch- oder vollautomatisierten Fahren bedurfte nach Einschätzung der Bundesregierung gesetzlicher Regelungen im Straßenverkehrsgesetz zum Zusammenwirken zwischen Fahrzeugführer und dem Kraftfahrzeug mit diesen weiterentwickelten Fahrfunktionen.

Der von der Bundesregierung im Februar 2017 vorgelegte Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT-Drs. 18/11300), der die rechtliche Grundlage für die Nutzung von hoch- oder vollautomatisierten Kraftfahrzeugen bilden sollte, war aus datenschutzrechtlicher Sicht völlig unzureichend. Eine Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. März 2017 benannte diese Defizite (**Anlage 14**).

In dem Gesetz vom 20. Juni 2017 (BGBl. I S. 1648) bleiben Haftungsfragen, Ethikaspekte und Anforderungen an einen Datenschutz durch Technikgestaltung unberücksichtigt.

Das Thema autonomes Fahren wird den Landesbeauftragten und insbesondere den Arbeitskreis Verkehr der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weiterhin beschäftigen. Das Thema ist nicht rein national begrenzt: So hat die 39. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in einer Entschließung[9] in Hongkong im September 2017 nähere rechtliche und technische Anforderungen bei der Nutzung automatisierter und vernetzter Fahrzeuge formuliert.

[9] https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Konferenzen/Internationale_Konferenz/hongkong2017_conference/2017_39thIDSK_HongKong_ResolutionOnDataProtectionAutomatedAndConnectedVehicles.pdf

Anlagen

Nationale Datenschutzkonferenz

Anlage 1

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, sodass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen

Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).

- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.

- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.

- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.

- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Anlage 2

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So sind dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.

- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.

- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.

- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.

- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.

- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.

- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.

- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

Anlage 3

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell[10], dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

[10] Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster; Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg; Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München; Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Anlage 4

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i. V. m. Erwägungsgrund [EG] 155),

- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i. V. m. EG 53, letzte beide Sätze),

- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i. V. m. EG 150, vorletzter Satz),

- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit,

Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),

- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),

- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

Anlage 5

Beschluss der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Vorschläge zu ersten Strukturfolgerungen aus der DSGVO

Unter der Annahme, dass

- die dem BDSG zugrunde liegende föderative Aufgabenverteilung insbesondere im nichtöffentlichen Bereich sich in einer nach der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) geforderten gesetzlichen Übergangsregelung wieder findet,
- eine rechtzeitige Einigung innerhalb der unabhängigen Aufsichtsbehörden (Datenschutzkonferenz – DSK) den Umsetzungsprozess der EU-DSGVO deutlich unterstützen würde,
- es auf europäischer Ebene wichtig ist, über längere Zeiträume personelle Kontinuität im Umgang mit den anderen europäischen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Europäischen Kommission zu ermöglichen,
- wegen der Sonderbedingungen der völligen Unabhängigkeit der beteiligten Behörden Vorbilder für die hierbei zu erfüllenden Regelungsaufgaben fehlen

macht die Konferenz folgende Vorschläge (vorbehaltlich etwaiger Zuständigkeiten und Befugnisse weiterer Aufsichtsbehörden, z. B. für Kirchen oder Rundfunkanstalten) für weitere Beratungen:

1. Grundsatzregelung

Innerhalb einer gesetzlichen Regelung sollte Folgendes geregelt werden:

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bilden einen Zusammenschluss (Datenschutzkonferenz). Unbeschadet der Regelungen unter Ziffer 3 regeln sie das Nähere autonom, insbesondere

- das Verfahren, mit dem sichergestellt wird, dass die Datenschutzaufsichtsbehörden in der Bundesrepublik Deutschland wirksam am Kohärenzverfahren nach der Europäischen Datenschutz-Grundverordnung teilnehmen,
- den innerstaatlichen Koordinierungs- und Abstimmungsprozess zur Mitwirkung im Europäischen Datenschutzausschuss
- die Bindungswirkung von Entscheidungen gegenüber der Vertretung im europäischen Datenschutzausschuss in Fällen des Art. 64 DSGVO
- die fachliche Verantwortlichkeit des Leiters der zentralen Kontaktstelle nach Erwägungsgrund 119 gegenüber den unabhängigen Datenschutzbehörden des Bundes und der Länder und die damit korrespondierende Weisungsbefugnis über die Kontaktstelle.

2. Vertretung im europäischen Datenschutzausschuss

Die DSK legt hierzu keinen Verfahrensvorschlag vor.

3. Zuständigkeiten und Beteiligungsverfahren

Zuständigkeitsregelungen sowie die Beteiligung in den Verfahren der Zusammenarbeit und der Kohärenz sind, soweit sie Außenwirkung entfalten, durch Gesetz zu treffen. Eine umfassende Zuständigkeitsregelung kann der Bundesgesetzgeber nicht treffen. Die Gesetzgebungskompetenz des Bundes aus Art. 84 Abs. 1, Satz 1 GG beschränkt sich auf den Vollzug von Bundesgesetzen. Auch die Landesgesetzgeber haben somit Zuständigkeitsregelungen zu treffen.

Für die Festlegung der Zuständigkeiten sind die folgenden Ansätze (laut Anlage) empfehlenswert. Sie haben das Ziel, soweit wie möglich eine bei einer Behörde konzentrierte Zuständigkeit zu erreichen und sich dabei an sachlichen Kriterien zu orientieren.

Damit ist im grenzüberschreitenden Fall häufig eine Abweichung vom Wortlaut der DSGVO verbunden. Ob dies mit den Vorgaben der DSGVO vereinbar ist, ist im Rahmen des Gesetzgebungsverfahrens zu prüfen.

Das Gesetz sollte sich darauf beschränken, die Aufsichtsbehörden zu verpflichten in den erforderlichen Fällen eine Abstimmung mit dem Ziel der einheitlichen Votierung vorzunehmen. Die Einzelheiten sollten die unabhängigen Aufsichtsbehörden autonom regeln.

4. Einrichtung einer zentralen Kontaktstelle

4.1. Anforderungen der Grundverordnung

Die EU-DSGVO berücksichtigt in Artikel 51 Abs. 3 (bisher: 46 Abs. 2) föderale Systeme der Mitgliedstaaten. Demnach hat jeder Mitgliedstaat, in dem es mehrere Aufsichtsbehörden gibt, eine Aufsichtsbehörde zu bestimmen, die alle Behörden im EDSA vertritt. Zusätzlich hat der Mitgliedstaat ein Verfahren einzuführen, mit dem sichergestellt ist, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 (bisher: 57) einhalten. In Artikel 51 Abs. 3 (bisher: 46 Abs. 2) ist nicht konkret von einer zentralen Kontaktstelle die Rede.

Der Erwägungsgrund 119 (bisher: 93) konkretisiert Artikel 51 Abs. 3 (bisher: 46 Abs. 2) jedoch. Der Mitgliedstaat hat sicherzustellen, dass die Aufsichtsbehörden im Kohärenzverfahren beteiligt werden und sollte zu diesem Zweck eine Aufsichtsbehörde bestimmen, die als zentrale Kontaktstelle für eine wirksame Beteiligung der Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit den anderen Aufsichtsbehörden, dem EDSA und der Kommission gewährleistet. Dabei muss es sich dem Wortlaut der genannten Regelungen nach nicht um dieselbe Aufsichtsbehörde handeln, wie in Artikel 51 Abs. 3 (bisher: 46 Abs. 2) vorgesehen ist. Die zentrale Kontaktstelle kann somit unabhängig von der vertretenden Aufsichtsbehörde im EDSA durch den Mitgliedstaat bestimmt werden.

Da der Erwägungsgrund 119 (bisher: 93) von einer Aufsichtsbehörde spricht, ist die Aufgabe der Kontaktstelle entweder einer bestehenden Aufsichtsbehörde der Länder

oder der Aufsichtsbehörde des Bundes zu übertragen. Dies hat der Gesetzgeber zu regeln.

4.2. Gestaltungsvorschlag:

4.2.1 Rechtsgrundlage der zentralen Anlaufstelle

Der Erwägungsgrund 119 (bisher: 93) sieht vor, dass der Mitgliedstaat durch ein Rechtsinstrument sicherstellt, dass die anderen Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. In diesem Gesetz ist festzulegen, dass eine zentrale Kontaktstelle i.S.v. Erwägungsgrund 119 (bisher: 93) errichtet wird und wo diese Kontaktstelle errichtet wird. Die Dienstaufsicht über das bei der Kontaktstelle beschäftigte Personal liegt bei der Aufsichtsbehörde, bei der die Kontaktstelle angesiedelt wird. Die Leitung der Kontaktstelle ist den unabhängigen Datenschutzbehörden des Bundes und der Länder gegenüber fachlich verantwortlich.

4.2.2 Ort der Kontaktstelle:

Die Kontaktstelle kann sowohl in Brüssel als auch in Deutschland errichtet werden. In Anbetracht der Lage und der Vernetzung liegt Brüssel als Standort nahe.

Gerade in den ersten Jahren der Anwendung der DSGVO werden eine Reihe wichtiger Entscheidungen vom Europäischen Datenschutzausschuss und von der Kommission getroffen, die sich auf Jahre hinaus auswirken und die künftige Auslegung und konkrete Umsetzung der DSGVO entscheidend prägen. Insofern ist es von enormer Bedeutung, dass die Aufsichtsbehörden aus Deutschland – dem größten Mitgliedstaat – ihr dezentral vorhandenes hohes Knowhow an zentraler Stelle bündeln und dort effektiv in die Entscheidungsprozesse einbringen können. Da alle maßgeblichen Entscheidungen in Brüssel vorbereitet und getroffen werden, bedarf es einer unmittelbaren und ständigen personellen Präsenz in Brüssel. Eine Kontaktstelle in Brüssel kann als zentrale Anlaufstelle für alle Europäischen Institutionen, Verbände und die Aufsichtsbehörden der anderen Mitgliedstaaten dienen und zugleich aktiv den unmittelbaren und persönlichen Kontakt zu allen Entscheidungsträgern herstellen und damit die Interessen der deutschen Aufsichtsbehörden im Sinne des Datenschutzes wirksam zur Geltung bringen.

Anlage 6

Beschluss der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016 in Schwerin

Anlage zu den Vorschlägen zu ersten Strukturfolgerungen aus der DSGVO

Fallkonstellation	Gesetzliche Zuständigkeitsregelung national und Abstimmungsverfahren Soweit die BfDI nicht allein zuständige Behörde ist (Post und Telekommunikation), bestehen folgende Zuständigkeiten der Aufsichtsbehörden der Länder insbesondere mit Blick auf den EU-Datenschutzausschuss:
1. Hauptniederlassung in Deutschland	• Aufsichtsbehörde am Ort der Hauptniederlassung • Aufsichtsbehörde am Ort der Hauptniederlassung ist auch zuständig für alle Eingaben, die ggf. an sie abgegeben werden müssen
2. Keine Hauptniederlassung in Deutschland, aber eine einzige Niederlassung (ggf. mit mehreren Betriebsstätten)	• Aufsichtsbehörde am Ort der Niederlassung (z. B. Eintragung ins Handelsregister) zuständig • keine Zuständigkeit der Aufsichtsbehörden am Ort weiterer Betriebsstätten, die keine Niederlassung sind • Aufsichtsbehörde i. S. d. ersten Anstrichs ist auch zuständig für alle Eingaben, die ggf. an sie abgegeben werden müssen
3.a) Keine Hauptniederlassung in Deutschland aber mehrere Niederlassungen, von denen eine einzige selbstständig ist	• Aufsichtsbehörde am Ort der selbstständigen Niederlassung örtlich zuständig

3. b) Keine Hauptniederlassung in Deutschland, aber mehrere Niederlassungen, von denen mehrere selbstständig sind	• Lokale Zuständigkeit jeweils am Ort einer selbstständigen Niederlassung • Bei mehreren zuständigen Aufsichtsbehörden treffen diese eine Zuständigkeitsvereinbarung. Soweit keine Einigung zustande kommt, findet eine Abstimmung auf Ebene der DSK statt.
3. c) Keine Hauptniederlassung in Deutschland, aber mehrere unselbstständige Niederlassungen	• Lokale Zuständigkeit jeweils am Ort einer unselbstständigen Niederlassung • Bei mehreren zuständigen Aufsichtsbehörden treffen diese eine Zuständigkeitsvereinbarung. Soweit keine Einigung zustande kommt, findet eine Abstimmung auf Ebene der DSK statt.
4. a) Keine Niederlassung in Deutschland, aber eine Eingabe	• Zuständigkeit der Aufsichtsbehörde, bei der die Eingabe eingeht
4. b) Keine Niederlassung in Deutschland, aber mehrere gleichartige Eingaben bei mehreren Aufsichtsbehörden	• Zuständigkeit jeweils der Aufsichtsbehörde, bei der Eingabe eingeht • Bei mehreren zuständigen Aufsichtsbehörden treffen diese eine Zuständigkeitsvereinbarung. Soweit keine Einigung zustande kommt, findet eine Abstimmung auf Ebene der DSK statt.
5. Keine Niederlassung in Deutschland bzw. Europa, keine Eingabe, aber Betroffenheit nach Art. 4 Abs. 22 (bisher. Abs. 19a) lit. b) DSGVO	• Grundsätzlich sind alle Bundesländer zuständig. Bei mehreren zuständigen Aufsichtsbehörden treffen diese eine Zuständigkeitsvereinbarung. Soweit keine Einigung zustande kommt, findet im Rahmen der DSK eine Abstimmung statt.

Anlage 7

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20. April 2016

Klagerecht für Datenschutzbehörden – EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU-US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können. Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in

der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6.10.2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

Anlage 8

Entschließung[11] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. Mai 2016

EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),

- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),

- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,

- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,

- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),

[11] bei Enthaltung Bayerns (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht)

- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,

- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,

- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

Anlage 9

Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 10. und 11. November 2016 in Kühlungsborn

Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf – Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[12] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

[12] bei Enthaltung Hamburgs

2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.
3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

Anlage 10

Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. November 2016 in Kühlungsborn

„Videoüberwachungsverbesserungsgesetz“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[13] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren di-

[13] bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

rekt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

Anlage 11

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 24. Januar 2017

Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.

- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten

aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.

- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

Anlage 12

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 15. März 2017

Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist.

Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

Anlage 13

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. März 2017

Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

Anlage 14

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. März 2017

Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,

- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,

- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,

- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,

- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,

- die Nennung des Adressaten für das Übermittlungsverlangen,

- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und

- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

Anlage 15

Entschließung der 93. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 29. und 30. März 2017 in Göttingen

Göttinger Erklärung – Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität“ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

Anlage 16

Entschließung der 93. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 29. und 30. März 2017 in Göttingen

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten“ erkannt werden soll.[14]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensi-

[14] Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“.

veren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

Anlage 17

Entschließung der 94. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 8. und 9. November 2017 in Oldenburg

Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records – PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visa-befreiten

Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

Anlage 18

Entschließung der 94. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 8. und 9. November 2017 in Oldenburg

Umsetzung der DSGVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i. V. m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DSGVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“. Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.

- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DSGVO).

- Die Grundsätze des Datenschutzes (Art. 5 DSGVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.

- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.

- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen i. S. d. Art. 85 DSGVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DSGVO – Ausnahmen und Abweichungen regeln und diese begründen.

- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

Anlage 19

Entschließung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. und 26. April 2018 in Düsseldorf

Facebook-Daten-Skandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftliche Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.

- Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.

- In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in

Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.

- Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

Anlage 20

Entschließung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. und 26. April 2018 in Düsseldorf

Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen

die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

Anlage 21

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. Juni 2018 in Düsseldorf

Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.

- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.

- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.

- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage- Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtliche Verantwortung nur erfüllen können, 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.

Anlage 22

Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23. März 2018

Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO

Die Zulässigkeit einer Einmeldung beurteilt sich künftig nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

Hierzu ist es notwendig, dass die Einmeldung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Zudem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Das bedeutet, dass eine Abwägung unter Berücksichtigung dieser Kriterien im Einzelfall vorzunehmen ist.

Im Rahmen dieser Einzelfallprüfung entfalten die nachfolgenden Fallgruppen eine Indizwirkung für eine zulässige Einmeldung:

1. Die Forderung ist durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden oder es liegt ein Schuldtitel nach § 794 der Zivilprozessordnung vor.

2. Die Forderung ist nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden.

3. Der Betroffene hat die Forderung ausdrücklich anerkannt.

4. Der Betroffene ist nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden, die erste Mahnung liegt mindestens vier Wochen zurück, der Betroffene ist zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden und der Betroffene hat die Forderung nicht bestritten.

5. Das der Forderung zugrunde liegende Vertragsverhältnis kann aufgrund von Zahlungsrückständen fristlos gekündigt werden und der Betroffene ist zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden.

Zusätzliche Anhaltspunkte oder Hinweise können ggf. zu einer anderen Abwägung führen.

Darüber hinaus muss eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO erfolgen, weil die personenbezogenen Daten zunächst für einen anderen Zweck – zur Durchführung eines Rechtsgeschäfts und nicht zur Einmeldung bei einer Auskunftei – verarbeitet wurden. Der Betroffene muss also zuvor durch die Auskunftei-Vertragspartner über die Möglichkeit der Einmeldung unterrichtet worden sein, denn es darf nur das eingemeldet werden, womit der Betroffene vernünftigerweise rechnen muss (Erwägungsgrund 47 der DS-GVO).

Anlage 23

Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23. März 2018

Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO grundsätzlich nur erteilen, wenn es zur Wahrung eines berechtigten Interesses eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen. Bei jeder dieser weiteren Auskünfte sind jedoch im Einzelfall die Voraussetzungen des Art. 6 Abs. 1 S. 1 lit. f DS-GVO strikt zu beachten. Das heißt vor jeder Übermittlung sind die konkreten berechtigten Interessen des Dritten gegen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person abzuwägen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen. Ein berechtigtes Interesse seitens des Versandhandels gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Anlage 24

Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 11. Juni 2018

Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien

Handels- und Wirtschaftsauskunfteien können sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 lit. f DS-GVO erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Daten nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür im Regelfall einer wirksamen Einwilligung der betroffenen Personen im Sinne des Art. 7 DS-GVO. Auf die hohen Anforderungen an die Freiwilligkeit nach Art. 7 Abs. 4 DS-GVO wird hingewiesen. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Besonderheiten für Kreditinstitute:

Es wird für zulässig angesehen, wenn Kreditinstitute aufgrund von Art. 6 Abs. 1 S. 1 lit. f DSGVO – wie bisher durch § 28 a Abs. 2 BDSG gesetzlich erlaubt – personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung von Kredit- und Giroverträgen sowie Garantiegeschäften (insbesondere Bürgschaften) an Auskunfteien übermitteln, es sei denn, dass im Einzelfall das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Übermittlung gegenüber den Interessen der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt.

Diese Besonderheit für Kreditinstitute begründet sich mit den speziellen Bonitätsprüfungsverpflichtungen der Kreditinstitute nach dem Kreditwesengesetz sowie gesamtgesellschaftlichen Gesichtspunkten des Schutzes der betroffenen Personen vor Überschuldung. Die betroffene Person ist vor Abschluss des Vertrages über die damit verbundene Datenübermittlung an Auskunfteien zu unterrichten.

Dies gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben.

Ebenso ist die Übermittlung von Daten zu allgemeinen Konditionenanfragen, die der Herstellung von Markttransparenz dienen, an Auskunfteien unzulässig; hierzu kann auch keine rechtswirksame Einwilligung der betroffenen Person eingeholt werden.

Die Übermittlung von Daten an Auskunfteien für Bonitätsabfragen ist nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig, wenn dies zur Durchführung eines Beratungsver-

trages oder einer vorvertraglichen Maßnahme, die auf Anfrage der betroffenen Person erfolgt, erforderlich ist mit dem Ziel, Konditionen, die auf eine bestimmte Person zugeschnittenen werden, zu überprüfen.

Nachträgliche Änderungen von Tatsachen hat das Kreditinstitut gemäß Art. 19 DS-GVO der Auskunftei unverzüglich nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat das betreffende Kreditinstitut über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

Zur Einmeldung von Dauerschuldverhältnissen außerhalb des KWG werden im AK Auskunfteien noch weitere Abstimmungen erfolgen.

Düsseldorfer Kreis

Anlage 25

Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis) vom 13. und 14. September 2016

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),

- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z