SACHSEN-ANHALT

XV. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Dieser Text entspricht der Landtagsdrucksache 7/4095

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

Vorwort

Der XV. Tätigkeitsbericht umfasst den Zeitraum vom 6. Mai 2018 bis zum 31. Dezember 2018. Bei einzelnen Beiträgen konnten noch darüber hinaus reichende aktuelle Sachstände einbezogen werden (Redaktionsschluss: 15. Februar 2019).

Der verkürzte Zeitraum und die Konzentration auf das Jahr 2018 beruhen auf dem Umstand, dass der Landesbeauftragte seit Mai 2018 zuständige Aufsichtsbehörde nach der Datenschutz-Grundverordnung (DS-GVO) und der JI-Richtlinie ist und diese Rechtsgrundlagen einen jährlichen Bericht vorgeben (vgl. auch Vorwort zum XIII./XIV. Tätigkeitsbericht).

Schwerpunkte dieses Berichts betreffen die Anwendung der DS-GVO für Unternehmen, Behörden und Betroffene. Auch werden aktuelle Gesetzgebungsvorhaben kommentiert. Schließlich geht es wieder um weitere Entwicklungen bei der Modernisierung und Digitalisierung von Verwaltung, Wirtschaft und Gesellschaft.

Der Bericht dient der Unterrichtung des Landtages, der Landesregierung und der verantwortlichen Stellen der Exekutive und allgemein der Öffentlichkeit. Auch die Europäische Kommission und der Europäische Datenschutzausschuss werden informiert.

Die Behörde ist durch den Aufgabenzuwachs infolge der DS-GVO stark beansprucht worden. Dies galt schon vor Beginn der verpflichtenden Anwendung der neuen Regelungen im Mai 2018. Trotz unzureichender Personalausstattung wurde weitgehend erreicht, das Land auf das neue Recht und dessen Anwendung vorzubereiten. Ich habe mich selbst dabei in der Verantwortung gesehen. Mein besonderer Dank gilt meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle.

Magdeburg, den 15. Februar 2019

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

Inhaltsverzeichnis

Anlagenverzeichnis

Abkürzungsverzeichnis

A

AK	Arbeitskreis
Art.	Artikel

B

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 2017 S. 2097)
beA	besonderes elektronisches Anwaltspostfach
BGBl.	Bundesgesetzblatt
BLSA	Landesbetrieb „Bau- und Liegenschaftsmanagement Sachsen-Anhalt“
BMG	Bundesmeldegesetz
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BZRG	Bundeszentralregistergesetz

C

CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer

D

DANE	DNS-based Authentication of Named Entities
DNS	Domain Name System
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA)
DSAnpG EU LSA	Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an das Recht der Europäischen Union (DSAnpG EU LSA)
DSAnpUG-EU	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DSUG LSA	Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzrichtlinienumsetzungsgesetz – DSUG LSA)
DS-GVO, DSGVO	Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der

	Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
E	
EDSA	Europäischer Datenschutzausschuss
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
ErwGr	Erwägungsgrund
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
E-Evidence-Verordnung	Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)
F	
FITKO	Föderale IT-Kooperation
G	
GG	Grundgesetz
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung
H	
I	
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
IPv6	Internet Protocol Version 6
ISM	Informationssicherheitsmanagement
ITN-XT	InformationsTechnischesNetz der nächsten Generation (neXT generation)
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
K	
KMU	kleine und mittlere Unternehmen
KunstUrhG	Kunsturhebergesetz
L	
LAN	Local Area Network

LISL LSA	Informationssicherheitsleitlinie Sachsen-Anhalt
LReg.	Landesregierung
LRZ	Landesrechenzentrum
LT-Drs.	Landtagsdrucksache

M

N

O

OZG	Onlinezugangsgesetz

P

Q

R

RdErl.	Runderlass

S

SGB V	Fünftes Buch Sozialgesetzbuch
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
s.	siehe

T

TLS	Transport Layer Security (Sicherheitsprotokoll)
TMG	Telemediengesetz

U

UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen
UWG	Gesetz gegen den unlauteren Wettbewerb

V

VEMAGS	Verfahrensmanagement für Großraum- und Schwertransporte
VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
vgl.	vergleiche

W

WAN	Wide Area Network

X

Y

Z

z. B.	zum Beispiel
ZAST	Zentrale Anlaufstelle
ZPO	Zivilprozessordnung

1 Einführung

1.1 Neuer Tätigkeitsbericht

Mit dem XV. Tätigkeitsbericht beginnt eine neue Art und Weise der Darstellung der Arbeit des Landesbeauftragten für den Datenschutz gemäß europarechtlichen Vorgaben. Der Landesbeauftragte ist eine völlig unabhängige Aufsichtsbehörde nach europäischem Recht.

Der Berichtszeitraum ist nunmehr auf ein Jahr verkürzt und ab dem Jahr 2019 auf das Kalenderjahr konzentriert.

Inhaltlich erfolgt auch dadurch eine Straffung im Sinne eines Rechenschaftsberichts unter Verzicht auf eine ausführliche Beschreibung jeglicher Einzelvorgänge.

Anders als nach alter Rechtslage wird der Bericht dem Landtag nicht mehr erstattet, sondern zur Unterrichtung übermittelt. Die Landesregierung muss zu diesem Bericht neuen Typs nicht mehr Stellung nehmen; die gesetzliche Verpflichtung hierzu ist entfallen.

Der Bericht wird auch der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

1.2 Entwicklung und Situation des Datenschutzes

Das Jahr 2018 war insgesamt durch das neue europäische Recht geprägt. Der Landesbeauftragte wirkte bei rechtspolitischen Entwicklungen mit und nahm vielfältige Beratungs- und Kontrollaufgaben hinsichtlich rechtspraktischer Anwendungsfragen und konkreter Datenverarbeitungsverstöße wahr. Der Landesbeauftragte handelt dabei als unabhängige Aufsichtsbehörde nach europäischem Recht.

Wie schon im XIII./XIV. Tätigkeitsbericht beschrieben, sind die Aufgaben und Befugnisse des Landesbeauftragten und seiner Geschäftsstelle qualitativ und quantitativ gewachsen. Der Umfang der Arbeitsfelder spiegelt dies wieder (Nr. 2.1). Die personelle Ausstattung der Aufsichtsbehörde reicht im Hinblick auf die Herausforderungen und Aufgaben infolge der DS-GVO nicht aus (Nr. 2.2).

Auch infolge der Medienberichterstattung über erste Erfahrungen mit der DS-GVO hat der Datenschutz allgemein eine breite gesellschaftliche Aufmerksamkeit erfahren. Allerdings führten manche Berichte über Missverständnisse und Irrtümer zu Verunsicherungen und Überreaktionen. Dies betraf etwa KMU und ehrenamtliche Vereinstätigkeiten.

Allerdings haben sich Unternehmen und Behörden insgesamt doch auf das neue Recht eingestellt und ihre Verfahren angepasst. Das neue europäische Recht, das in vielen Details gar nicht so neu ist und gerade in Deutschland bekannte Regelungen abbildet, findet trotz eines gewissen zusätzlichen Aufwandes mehr und mehr Akzeptanz. Gerade betroffene Verbraucherinnen und Verbraucher und Bürgerinnen und Bürger sind stärker sensibilisiert und profitieren von ihren Rechten. Die Zusammenarbeit unter den europäischen Datenschutzaufsichtsbehörden entwickelt sich stetig und gewinnt an Effektivität. Einzelne Kritikpunkte an der DS-GVO, aber auch am BDSG 2018, etwa im Hinblick auf zu viel Bürokratisierung, werden im Rahmen von

Evaluierungen aufzugreifen sein; die DSK beteiligt sich an diesen Prozessen. Allerdings versteckt sich hinter mancher Kritik an der DS-GVO und deren angeblicher Überregulierung eine eher grundsätzliche Verweigerung bis hin zur Ablehnung des Datenschutzes. Diese Gesichtspunkte spiegelten sich auch in den Beiträgen der Veranstaltung der DSK zum 13. Europäischen Datenschutztag („Europäischer Datenschutz: Chance oder Risiko? Acht Monate DS-GVO – Bilanz und Blick nach vorn.“) am 28. Januar 2019 in Berlin wieder.

Aktuelle Ereignisse und Entwicklungen der Digitalisierung von Wirtschaft, Verwaltung und Gesellschaft fordern den Datenschutz in besonderer Weise heraus. Dies betrifft etwa Datenskandale durch Hacker-Angriffe (Doxing-Vorgänge „Adventskalender“, Password-Leaks „Collections“) und Informationssicherheitspannen großen Ausmaßes. Dies gilt aber auch für die neuen Geschäftsmodelle mittels Künstlicher Intelligenz. Die KI-Aspekte hat der Landesbeauftragte bereits im Vorgängerbericht beschrieben (Nr. 1.2; vgl. zu den vielen aktuellen Positionsbestimmungen beispielhaft die Strategie der Bundesregierung zu KI vom November 2018 in BT-Drs. 19/5880).

Die DSK hat neben den vielen Auslegungsfragen der DS-GVO auch diese Entwicklungen im Blick. Die DS-GVO selbst gibt mit dem Grundsatz „Data Protection by Design“ (Datenschutz durch Technikgestaltung) und der Forderung nach Datenminimierung bis hin zur Anonymisierung eine wesentliche Antwort, die über reine ethische Überlegungen hinausgeht. Datenschutz stellt grundsätzlich kein Hindernis für Digitalisierungsvorhaben dar, sondern ist als zentraler Grundrechtsmaßstab wesentlicher Faktor für deren Gelingen. Digitalisierung darf nicht als Selbstzweck, sondern muss als dienendes Mittel zum Wohle des Menschen verstanden werden. Datenschutz bleibt essentiell für eine moderne Gesellschaft und ein demokratisches Gemeinwesen.

Wer trägt die Verantwortung für die Wahrung von Privatheit und Datenschutz?
Der einzelne Bürger bzw. Internet-Nutzer? Ja! (Selbstdatenschutz!)
Die Unternehmen und Datensammler? Ja! (DS-GVO)
Der Staat? Ja! (DS-GVO und Grundrechtsschutzaufgabe)
Die Datenschutzaufsichtsbehörden? Ja! (DS-GVO)

Aus den Überlegungen ergeben sich auch neue strategische Fragen, z. B. zur Durchsetzung des internationalen Rechts. Auch ist es zwingend, dass der Staat sein eigenes, widersprüchliches Verhalten aufgibt, wenn er etwa Datensicherheit fordert und gleichzeitig Sicherheitslücken ausnutzt und nicht schließen lässt.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Der Landesbeauftragte ist aufgrund der DS-GVO und der JI-Richtlinie (vgl. Nr. 4.1) gemäß dem Landesgesetz zur Organisationsfortentwicklung des Landesbeauftragten eine Datenschutzaufsichtsbehörde nach europäischem Recht geworden. Hiermit sind alte und neue Aufgaben und Befugnisse verbunden. Diese betreffen im Wesentlichen:

- Aufsicht gegenüber Unternehmen und Behörden,
- Beratung von Betroffenen, Unternehmen und Behörden,
- Beratung des Landesgesetzgebers,
- Kooperation mit anderen Aufsichtsbehörden in Deutschland und in der EU,
- Sensibilisierung der Öffentlichkeit.

Schwerpunkte: Beratung, Information, Kontrolle

Die Tätigkeit im Berichtszeitraum war wesentlich geprägt von der neuen Rechtslage im Datenschutz seit dem 25. Mai 2018. Besonders großen Wert legte der Landesbeauftragte auf die Bereitstellung von Informationen für Verantwortliche im öffentlichen und nichtöffentlichen Bereich sowie für betroffene Personen. Dazu hat er eine Fülle von Beschwerden und Informationsanfragen schriftlich beantwortet und mündliche Beratungen durchgeführt (Zahlen und Fakten siehe Kapitel 3). Besonders viele Eingaben bezogen sich auf die Rechtsgrundlagen für die Datenverarbeitung, die Informationspflichten, die Betroffenenrechte, die Pflicht zur Benennung von Datenschutzbeauftragten und die Auftragsverarbeitung.

Aufgrund zahlreicher Anfragen von Unternehmensverbänden, berufsständischen Kammern, Vereinen und Bildungseinrichtungen hielten der Landesbeauftragte und seine Mitarbeiter zahlreiche Vorträge zu unterschiedlichen Bereichen des neuen Datenschutzrechts.

Auch gegenüber öffentlichen Stellen wurde in einer Vielzahl von Vorträgen, Veranstaltungen und Beratungen die komplexe Rechtslage erläutert. Denn bis zum Inkrafttreten des Datenschutz-Grundverordnungs-Ausfüllungsgesetzes Sachsen-Anhalt (DSAG LSA) gilt das Datenschutzgesetz Sachsen-Anhalt (DSG LSA) weiter. Einige Vorschriften des DSG LSA sind aber wegen der Vorrangigkeit der DS-GVO nicht mehr anzuwenden. Den Anfragen vieler Behörden und Einrichtungen konnte im Rahmen der vorhandenen Kapazitäten entsprochen werden. Einbezogen wurden u. a. Ministerien, Landesämter, Kommunen, Zweckverbände, Kammern, Innungen und ärztliche Vereinigungen sowie der Verband Deutscher Privatschulen Sachsen-Anhalt. Mit den Hochschuldatenschutzbeauftragten fand die jährliche Beratungsrunde auch zu Themenschwerpunkten aus der DS-GVO statt.

Der alljährliche Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der Landkreise und der kreisfreien Städte konnte aufgrund der hohen Arbeitsbelastung erst im Januar 2019 durchgeführt werden.

Weiter wurden die Fortbildungen des Aus- und Fortbildungsinstituts des Landes mit Dozententätigkeiten unterstützt.

Der Gesamtaufwand der Befassung mit den Neuerungen der DS-GVO wirkte sich negativ auf den Umfang der Kontrolltätigkeit des Landesbeauftragten aus. Anlassunabhängige Kontrollen konnten im Berichtszeitraum daher nicht durchgeführt werden. Im Rahmen von Beschwerden mussten allerdings erste verwaltungsrechtliche Anordnungen erlassen und Bußgeldverfahren eingeleitet werden.

Öffentlichkeitsarbeit

Zur Sensibilisierung der Öffentlichkeit dient neben den vielen Beratungen und Veranstaltungen auch das Informationsangebot des Landesbeauftragten auf seiner Homepage. Zu den dem Landesbeauftragten häufig gestellten Fragen publizierte er u. a. eigene Informationen:

- einen Fragenkatalog zur DS-GVO insbesondere für kleine und mittlere Unternehmen,
- häufig gestellte Fragen (und Antworten) zum Datenschutz in Vereinen,
- Hinweise zu Rechtsgrundlagen für die Datenverarbeitung und die Informationspflichten für (Zahn-)Arztpraxen,
- eine Checkliste zur Dokumentation technischer und organisatorischer Maßnahmen und
- ein Informationsblatt zum Datenträgerschutz.

Weitere Veröffentlichungen werden vorbereitet.

Der Landesbeauftragte hat die o. g. Checkliste zur Dokumentation und zur Selbstkontrolle der getroffenen technischen und organisatorischen Maßnahmen erarbeitet, die sich aus den Anforderungen aus Art. 5, 24, 25 und 32 DS-GVO ergeben. Diese dient der Unterstützung des Verantwortlichen und des Auftragsverarbeiters. Sie kann auch u. a. als Anlage bei Verträgen der Auftragsverarbeitung (Art. 28 DS-GVO) und dem Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) Verwendung finden. Die Checkliste enthält auch Angaben zur Protokollierung als Maßnahme zur Revisionsfähigkeit, die sich im neuen europäischen Recht im Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DS-GVO manifestiert.

Auf seiner Homepage werden darüber hinaus Informationsmaterialien der DSK[1] (z. B. Auslegungshilfen in Form von Kurzpapieren) und auch des Europäischen Datenschutzausschusses (EDSA) veröffentlicht.

Kooperation der europäischen Aufsichtsbehörden, EDSA

Eine wichtige Neuerung der DS-GVO ist die Art und Weise, wie die Aufsichtsbehörden der Mitgliedstaaten in grenzüberschreitenden Fällen zusammenarbeiten, um eine einheitliche Anwendung des Rechts und einen einheitlichen Schutz von Personen in der gesamten EU zu gewährleisten.

Durch die Einführung des sog. „One-Stop-Shop-Prinzips“ ist bei grenzüberschreitenden Datenverarbeitungen für Unternehmen und deren Tochtergesellschaften nur noch eine federführende Aufsichtsbehörde am Sitz der „Hauptniederlassung” des Verantwortlichen oder des Auftragsverarbeiters zuständig (Art. 56 Abs. 1 DS-GVO). Sie muss ihre Entscheidung mit den anderen betroffenen Aufsichtsbehörden abstimmen (Art. 60 ff. DS-GVO), welche relevante und begründete Einwände gegen den Entscheidungsentwurf vorbringen können.

[1] Die DSK hat eine eigene Homepage eingerichtet: https://www.datenschutzkonferenz-online.de/

Soweit eine Einigung auf die Vorgehensweise zwischen der federführenden und der betroffenen Aufsichtsbehörde erzielt wird, ergeht ein entsprechender Beschluss durch die federführende Aufsichtsbehörde an die Hauptniederlassung des Verantwortlichen. Der Beschwerdeführer wird von der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, über den Beschluss informiert (Art. 60 Abs. 7 DS-GVO).

In den Fällen des „One-Stop-Shop“, bei denen das Verfahren über die Zusammenarbeit zu keiner Einigung geführt hat, ist das sog. Kohärenzverfahren einzuleiten. In diesem wird der Streit durch einen verbindlichen Beschluss des EDSA gemäß Art. 65 Abs. 1 lit. a DS-GVO beigelegt. Die federführende Aufsichtsbehörde erlässt ihre endgültige Entscheidung auf der Grundlage der verbindlichen Entscheidung des EDSA.

Durch die Einrichtung des EDSA, der aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten besteht, will die DS-GVO eine einheitliche Rechtsdurchsetzung und -anwendung in Europa gewährleisten.

Neben Stellungnahmen und Beschlüssen zu bestimmten beabsichtigten Maßnahmen der Aufsichtsbehörden in Einzelfällen stellt der EDSA u. a. allgemeine Anleitungen wie Leitlinien, Empfehlungen und bewährte Verfahren bereit, prüft deren praktische Anwendung und berät die EU-Kommission in allen Fragen des Datenschutzes (Art. 70 DS-GVO). Hierzu existieren diverse Facharbeitsgruppen (sog. Expert Subgroups), an deren Beratungen auch die deutschen Aufsichtsbehörden intensiv beteiligt sind.

Binnenmarkt-Informationssystem (IMI)

Das Binnenmarkt-Informationssystem (IMI) ist die IT-Plattform, die zur Unterstützung der Zusammenarbeit und Kohärenz im Rahmen der DS-GVO gewählt wurde. Die Aufsichtsbehörden der Mitgliedstaaten organisieren über die IMI-Plattform die gegenseitige Amtshilfe und die Koordinierung der Entscheidungsfindung in grenzüberschreitenden Datenschutzfällen elektronisch. Mit IMI können die Aufsichtsbehörden u. a.:

- die federführende Aufsichtsbehörde in einem grenzüberschreitenden Fall ermitteln,
- gemeinsam an der Lösung grenzüberschreitender Fälle arbeiten,
- die Aufsichtsbehörden anderer Mitgliedstaaten um Unterstützung bitten oder ihnen Hilfe anbieten,
- gemeinsame Aktionen unter Beteiligung der Aufsichtsbehörden mehrerer Mitgliedstaaten organisieren,
- den EDSA konsultieren und um eine Stellungnahme oder einen verbindlichen Beschluss ersuchen.

Hierzu bietet IMI formularähnliche Eingabemasken und automatisierte, termingestützte Verfahren an. Die Arbeitssprache ist Englisch. Die beteiligten Aufsichtsbehörden werden über jeden Verfahrensschritt per E-Mail informiert.

Zentrale Anlaufstelle (ZAST)

Aufgrund des föderalen deutschen Systems mit dem Datenschutzbeauftragten des Bundes und insgesamt 17 Datenschutzaufsichtsbehörden der Länder musste eine

„Zentrale Anlaufstelle“ bestimmt werden, um eine wirksame Beteiligung der deutschen Aufsichtsbehörden am Kohärenzverfahren sowie ihre rasche und reibungslose Zusammenarbeit im europäischen Kontext zu gewährleisten (Art. 51 Abs. 3 i. V. m. ErwGr 119). Die ZAST soll es den Aufsichtsbehörden der anderen Mitgliedstaaten, dem EDSA und der EU-Kommission ermöglichen, ohne Kenntnis der innerstaatlichen Zuständigkeitsverteilung effektiv mit den deutschen Aufsichtsbehörden zu kommunizieren.

Der deutsche Gesetzgeber hat die Funktion der ZAST nach § 17 BDSG 2018 dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zugewiesen. Die kommunikativen Aufgaben der ZAST betreffen zumindest alle in der DS-GVO geregelten formalen Zusammenarbeitsverfahren wie z. B. die Übermittlung von zweckdienlichen Informationen, von Beschlussentwürfen zu Einsprüchen gegen Entscheidungsvorschläge anderer Aufsichtsbehörden oder von Amtshilfeersuchen, aber auch formaler Positionsbestimmungen der deutschen Aufsichtsbehörden an den EDSA im Rahmen des Kohärenzverfahrens und der Festlegung von Leitlinien zur Auslegung der DS-GVO.

In diesem Zusammenhang kommen der ZAST auch unterstützende und koordinierende Aufgaben zu, wie z. B. die Kontrolle der für die Verfahren nach DS-GVO vorgesehenen Fristen oder die Begleitung der Erarbeitung gemeinsamer Standpunkte der deutschen Datenschutzaufsichtsbehörden in europäischen Angelegenheiten. Dies berührt auch die Abstimmungen und Kooperationen im Rahmen der nationalen Datenschutzkonferenz.

Datenschutzkonferenz

Die Zusammenarbeit der Datenschutzaufsichtsbehörden in der Datenschutzkonferenz hat nicht nur durch die Arbeit mit der ZAST erheblich an Umfang zugenommen. Vielfältige neue Fragen im Zusammenhang mit der Interpretation und Anwendung der DS-GVO machen weiterhin eine höhere Anzahl von Konferenzen und Sitzungen der Arbeitskreise notwendig, an denen sich der Landesbeauftragte bzw. Mitarbeiter und Mitarbeiterinnen der Geschäftsstelle regelmäßig beteiligen. Dies schließt die Befassung mit den Entwicklungen der Digitalen Gesellschaft ein.

2.2 Unzureichende Personalausstattung der Geschäftsstelle

Der Landesbeauftragte hat in seinem XIII./XIV. Tätigkeitsbericht (Nr. 2.3) die Problematik der unzureichenden Personalausstattung der Geschäftsstelle ausführlich beschrieben.

Für den Doppelhaushalt des Landes 2017/2018 wurden von 16 angemeldeten Stellen lediglich 4 Stellen bewilligt.

Für den Haushalt 2019 wurden die nicht bewilligten und daher fehlenden 12 Stellen erneut angemeldet.

Das Ministerium der Finanzen (MF) kürzte diese Anmeldung im Rahmen der Haushaltsaufstellung einseitig und willkürlich auf 4 Stellen herunter.

Der Landesbeauftragte wurde hierzu nicht beteiligt. Zur Begründung wurde seitens der Landesregierung auf Nachfrage des Landesbeauftragten mitgeteilt, dass sämtli-

che Ressorts Einsparungen erbringen müssten und hierzu mit den Ressortministern Gespräche geführt worden seien.

Der Landesbeauftragte widersprach dieser Aussage, da er mit seiner Geschäftsstelle völlig unabhängig und nicht einem Fachressort der Landesregierung vergleichbar sei. Vielmehr sei eine Vergleichbarkeit mit dem Landesrechnungshof oder dem Landtag gegeben, deren Haushaltsanmeldungen ohne Eingriffe des MF dem Landtag vorgelegt werden.

Der Landesbeauftragte wies auf die europarechtlich verbindlichen Vorgaben aus Art. 52 DS-GVO hinsichtlich der völligen Unabhängigkeit und der Sicherstellung der personellen und finanziellen Ressourcen hin (Hinweis: Dies hat nichts mit der eingeschränkten Finanzkontrolle der Aufsichtsbehörde durch den Landesrechnungshof im Sinne des Art. 52 Abs. 6 DS-GVO zu tun.).

In den Beratungen des Landtagsausschusses für Finanzen zum Einzelplan 18 des Landesbeauftragten rügte der Landesbeauftragte erneut den europarechtlich unzulässigen Eingriff in seine Unabhängigkeit durch das einseitige Abändern seiner Haushaltsanmeldung. Das MF verwies darauf, dass die Aufsichtsbehörden in anderen Ländern auch nicht mehr Stellen hätten. Dabei ignoriert die Landesregierung, dass auch den anderen Aufsichtsbehörden zu wenig Stellen zur Verfügung gestellt wurden.

Der Ausschuss griff die Mehranmeldung von zusätzlichen 8 Stellen nicht gesondert auf.

Im Ergebnis bewilligte der Landtag lediglich die 4 Stellen, die das MF in den Haushaltsentwurf aufgenommen hatte.

Infolgedessen stehen dem Landesbeauftragten von den ursprünglich angemeldeten 16 Stellen nur 8 neue Stellen zur Verfügung. Damit kann eine vollständige Aufgabenwahrnehmung (s. auch Nr. 2.1) nicht gewährleistet werden.

Das Gutachten zum „zusätzlichen Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung“ von Herrn Prof. Dr. Alexander Roßnagel (s. XIII./XIV. Tätigkeitsbericht, Nr. 2.3) hatte den Mehrbedarf – für den Kernbereich der Aufgaben nach der DS-GVO – bereits auf zusätzliche 28 Stellen beziffert.

Darüber hinaus ist zu beachten, dass der Landesbeauftragte mit der Verselbständigung seiner Behörde auch zusätzliche Binnenaufgaben in den Bereichen von Personal, Haushalt und Organisation eigenständig wahrnehmen muss.

Die unzureichende Personalausstattung der Geschäftsstelle hat – zumal infolge der Mehrbelastungen durch die DS-GVO (s. Kapitel 3) – bereits zu spürbaren Einschränkungen und Verzögerungen der Aufgabenwahrnehmungen und damit zu weiteren Eingriffen in die Unabhängigkeit geführt. Dies betrifft beispielsweise die Bearbeitung von Beschwerden und Anfragen, auch den Bereich von JI-Richtlinie und Polizei, und schließlich Aktivitäten zur Aufklärung der Bevölkerung über Risiken, Vorschriften, Garantien und Rechte bei Datenverarbeitungen und neue Entwicklungen im Rahmen der Digitalisierung der Gesellschaft.

Die Politik betont gern den Wert eines modernen Datenschutzes. Doch wird dieser Anspruch bei der Personalausstattung der unabhängigen Aufsichtsbehörde missachtet. Datenschutz verdient in der Landespolitik einen größeren Stellenwert.

3 Zahlen und Fakten

Die Geschäftseingänge der Behörde entwickelten sich wie folgt:

2015: 5.230 2016: 5.506 2017: 6.737 2018: 12.908

Bei der Zahl für 2018 ist zu berücksichtigen, dass diese das gesamte Jahr umfasst und die Mitteilungen der Verantwortlichen und Auftragsverarbeiter gem. Art. 37 Abs. 7 DS-GVO über die Benennung eines Datenschutzbeauftragten einschließt.

Die nachfolgenden Daten wurden statistisch für den Zeitraum vom 15. Juni bis 31. Dezember 2018 erfasst.

Beschwerden und Eingaben	**358**
Informations- und Beratungsfälle (schriftlich wie mündlich; bereits in den Vormonaten wurden Beratungen in erheblichem Umfang durchgeführt)	**789**
Vorträge und Veranstaltungen (vgl. Nr. 2.1)	**31**
Meldungen von Datenschutzverletzungen	**53**
Abhilfemaßnahmen/Anordnungen (einschl. Bußgeldverfahren)	**10**
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz – vgl. Nr. 2.1)	**5**
Förmliche Begleitung von Rechtsetzungsvorhaben	**14**

Ressourcen: **24,5** Stellen (einschließlich Landesbeauftragter – vgl. Nr. 2.2)

Viele Beratungen erfolgten ausführlich unmittelbar am Telefon, insbesondere gegenüber Unternehmen. Auf diese Weise gelang es, durch Hinweise auf die neue Rechtslage und deren Beachtung in der Rechtspraxis im Vorfeld mögliche Datenschutzverstöße zu vermeiden. Dadurch wurde es in vielen Fällen auch nicht nötig, Abhilfemaßnahmen anzuordnen.

Bei den statistischen Angaben ist zu berücksichtigen, dass der Erfassungszeitraum lediglich ein halbes Jahr wiederspiegelt und viele Eingaben und Beschwerden im Berichtszeitraum noch nicht abgeschlossen werden konnten. Dies ist auch der unzureichenden Personalausstattung geschuldet.

4 Nationales und internationales Datenschutzrecht

4.1 Neue Rechtsgrundlagen im Landesrecht

4.1.1 Anpassung an die Datenschutz-Grundverordnung

In den Beiträgen Nr. 3.1.1 des XI. und des XII. Tätigkeitsberichts hat der Landesbeauftragte auf die Europäische Datenschutz-Grundverordnung hingewiesen und die zu erwartenden Entwicklungen und wesentlichen Änderungen beschrieben. Im XIII./XIV. Tätigkeitsbericht (Nr. 3.1.1) erfolgten weitere Darlegungen zur seit dem 25. Mai 2018 geltenden Datenschutz-Grundverordnung. Daneben waren und sind jedoch weitere Neuerungen zu beachten: Das neue Bundesdatenschutzgesetz (Nr. 3.1.3), die Anpassung des Datenschutzrechts des Landes (Nr. 3.1.4).

Zur Ergänzung der Datenschutz-Grundverordnung ist ein Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an das Recht der Europäischen Union (DSAnpG EU LSA) geplant. Der Entwurf liegt seit Mitte Januar 2019 als LT-Drs. 7/3826 vor. Das Gesetz soll ausfüllende und ausführende Regelungen zur Datenschutz-Grundverordnung enthalten und durch Änderungen in einigen Fachgesetzen das bereichsspezifische Recht im Verantwortungsbereich des Ministeriums für Inneres und Sport anpassen. Damit wird von der Befugnis nach Art. 6 Abs. 1 lit. e, Abs. 2 und 3 DS-GVO zur Einführung bzw. Beibehaltung von spezifischen Bestimmungen und zu Anpassungsregelungen zur Erfüllung von klassischen Staatsaufgaben durch öffentliche Stellen in Sachsen-Anhalt Gebrauch gemacht.

Wesentlicher Bestandteil dieses Gesetzes ist in Artikel 1 der Entwurf eines Gesetzes zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA). Dieses Gesetz löst das DSG LSA ab. Das DSAG LSA enthält u. a. allgemeine Rechtsgrundlagen für Datenverarbeitungen öffentlicher Stellen und Beschränkungen von Betroffenenrechten. Weiter trifft der Entwurf sowohl für den Bereich der Datenschutz-Grundverordnung als auch für den Richtlinienbereich (Richtlinie (EU) 2016/680, siehe Art. 32 bis 34 und Art. 41 bis 49) Regelungen zur Datenschutzaufsicht und zum behördlichen Datenschutzbeauftragten.

Der Gesetzentwurf der Landesregierung wurde im September 2018 zur Anhörung freigegeben. Der Landesbeauftragte ist bereits im Vorfeld vom Ministerium für Inneres und Sport umfänglich beteiligt worden und war schriftlich und in vielen Gesprächen beratend tätig. Auch im Rahmen der Anhörung hat er auf einige noch verbesserungsfähige Aspekte, etwa zur Verarbeitung besonderer Kategorien von personenbezogenen Daten, hingewiesen (vgl. zu Details LT-Drs. 7/3826).

Das Landesrecht bedarf daneben vielfach weiterer fachrechtlicher Anpassungen, die seit dem 25. Mai 2018 überfällig sind. In dem fortbestehenden Interministeriellen Arbeitskreis Datenschutz ist der Landesbeauftragte weiterhin beratend tätig.

4.1.2 Umsetzung der JI-Richtlinie

Wie bereits im XIII./XIV. Tätigkeitsbericht (Nr. 3.1.4) dargestellt, ist als weiterer Schritt zur Anpassung des Landesdatenschutzrechts an die europäischen Vorgaben

eine Regelung zur Umsetzung der sog. JI-Richtlinie vorgesehen. Hierzu brachte die Landesregierung Ende Juli 2018 einen Entwurf eines 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 in den Landtag ein (LT-Drs. 7/3207). Der Entwurf dient der Umsetzung der Richtlinienvorgaben zur Verarbeitung von personenbezogenen Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, einschließlich dazu erfolgender Gefahrenabwehrmaßnahmen, sowie auch der Datenverarbeitung zum Zweck der Verfolgung von Ordnungswidrigkeiten. Der Entwurf umfasst insbesondere in Artikel 1 das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt – DSUG LSA) und in Artikel 3 Änderungen des SOG LSA (s. Nr. 7.1).

Der Landesbeauftragte hatte bereits in mehreren Gesprächen gegenüber dem Ministerium für Inneres und Sport Anregungen gegeben, die in den Entwurf Eingang fanden. Weiter wurden Hinweise aufgegriffen, die im Rahmen der Anhörung der Landesregierung erfolgten (s. zu Details LT-Drs. 7/3207). Ergänzend hat der Landesbeauftragte auch auf Bitten des Ausschusses für Inneres und Sport des Landtags von Sachsen-Anhalt Stellung genommen. Unter anderem wurde erneut darauf hingewiesen, dass eine allgemeine Rechtsgrundlage für notwendige Verarbeitungen fehlt, für die keine bereichsspezifischen Regelungen getroffen werden. Zur vorgesehenen Vorschrift zur Verarbeitung von Daten für Forschungszwecke wurde kritisiert, dass sie den Betroffenenrechten nicht in hinreichendem Umfang Rechnung trägt.

Bei Redaktionsschluss dauerten die Beratungen in den Landtagsausschüssen noch an.

4.2 Parlament und Datenschutz-Grundverordnung

Nach Art. 2 Abs. 2 lit. a DS-GVO findet die Grundverordnung keine Anwendung für Datenverarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen. Der Bereich der Willensbildung des Volkes und der hierfür vorgesehenen Einrichtungen und Organe, also die parlamentarische Kerntätigkeit, gehört nicht zu den der Union zugewiesenen Aufgabenkreisen. Insoweit ist hier ein Bereich betroffen, der nicht in den Anwendungsbereich des Unionsrechts und damit nicht unter die DS-GVO fällt. Dagegen kann für Aktivitäten von Abgeordneten oder Fraktionen, wenn sie reine Verwaltungstätigkeiten darstellen (z. B. Beschäftigung von Personal), die DS-GVO gelten. Auf Vorschlag des Landesbeauftragten hat sich die Datenschutzkonferenz mit der Problematik befasst und für die Rechtspraxis einige Positionierungen als Grundlage weiterer Bewertungen empfohlen:

Soweit Datenverarbeitungen von Parlamenten (auch durch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die DS-GVO keine Anwendung. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt. Die Einordnung von Tätigkeiten als verwaltende und fiskalische, die der DS-GVO unterlägen, bedarf jeweils einer Bewertung im Einzelfall. Parteien sind dagegen als nichtöffentli-

che Stellen grundsätzlich Normadressaten der DS-GVO und unterliegen damit der Aufsicht durch die Aufsichtsbehörden.

Der Beschluss der Datenschutzkonferenz „Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien“ vom 5. September 2018 (**Anlage 4**) ist auf der Homepage des Landesbeauftragten veröffentlicht.

Der Landesbeauftragte orientiert sich in seiner Beratungspraxis an diesen Grundsätzen. Soweit etwa Fraktionen im Bereich parlamentarischer Kerntätigkeit Datenverarbeitungen vornehmen, besteht aber kein rechtsfreier Raum. Betroffene können grundrechtsunmittelbare Ansprüche ggf. gerichtlich geltend machen.

4.3 Anpassungen im Bundesrecht

Im XIII./XIV. Tätigkeitsbericht (Nr. 3.1.3) hat der Landesbeauftragte auf das (erste) 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) hingewiesen, dessen wesentlicher Bestandteil das neue BDSG darstellt. Inzwischen liegt mit der BT-Drs. 19/4674 vom 1. Oktober 2018 der Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. DSAnpUG-EU) vor. In den einzelnen Artikeln dieses Entwurfs sind bereichsspezifische Änderungen in 154 Einzelgesetzen vorgesehen (u. a. Beamtenstatusgesetz, E-Government-Gesetz, Personenstandsgesetz, Strafgesetzbuch, Abgabenordnung, Gewerbeordnung, SGB II bis XII).

Im Wesentlichen enthalten die Regelungen Anpassungen in der Terminologie und den Verweisungen. Aber auch einige materielle Regelungen sind enthalten. So werden z. B. in einzelnen Regelungen die Betroffenenrechte u. a. auf Auskunft sehr weitreichend eingeschränkt. Zusätzlich sind Anpassungen aufgrund der Vorgaben der DS-GVO im Bereich technisch-organisatorischer Maßnahmen vorgesehen. Darüber hinaus sollen Änderungen im BDSG Datenverarbeitungen zu Zwecken staatlicher Auszeichnungen und Ehrungen normieren und die Voraussetzung schaffen, dass zivilgesellschaftliche Träger im Rahmen von Deradikalisierungsprogrammen notwendige sensible Daten verarbeiten dürfen.

4.4 Weitere europäische und internationale Entwicklungen

4.4.1 Privacy Shield

Die Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWRs ist nach der DS-GVO zulässig, wenn die EU-Kommission die Angemessenheit des Datenschutzniveaus im Empfängerland nach Art. 45 DS-GVO festgestellt hat oder wenn die in Art. 46 Abs. 2 und 3 DS-GVO genannten Garantien (z. B. Standard-Datenschutzklauseln) vorliegen. In bestimmten Fällen können solche Übermittlungen auch nach den Ausnahmeregelungen des Art. 49 DS-GVO (z. B. Einwilligung) zulässig sein.

Mit Beschluss vom 12. Juli 2016 hatte die Europäische Kommission in Bezug auf die Übermittlung personenbezogener Daten von Unternehmen aus einem Mitgliedstaat der Europäischen Union in die USA entschieden, dass das EU-U.S. Privacy Shield

hierfür ein angemessenes Schutzniveau gewährleistet. Das übermittelnde Unternehmen muss nach den Regelungen des EU-U.S. Privacy Shield zertifiziert sein. Auf die am Privacy Shield geäußerte Kritik hatte der Landesbeauftragte in seinem XIII./XIV. Tätigkeitsbericht (Nr. 3.2.1) hingewiesen.

Das Ergebnis der Überprüfung des EU-U.S. Privacy Shield durch die EU-Kommission im Jahre 2018 bewertete der Europäische Datenschutzausschuss Ende Januar 2019 durchaus skeptisch, insbesondere im Hinblick auf die noch fehlende Ernennung einer ständigen Ombudsperson und deren Befugnisse. Auch äußerte der Europäische Datenschutzausschuss nach wie vor Bedenken, beispielsweise über das Fehlen von Zusicherungen, die einen wahllosen Zugriff auf personenbezogene Daten zu Zwecken der nationalen Sicherheit ausschließen.

4.4.2 Internationale Datenschutzkonferenz

Im Berichtszeitraum fand am 23. Oktober 2018 in Brüssel die 40. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre statt. Der Teilnehmerkreis umfasste neben Vertretern nationaler Datenschutzbehörden auch Vertreter nichtstaatlicher und internationaler Organisationen sowie Vertreter aus Wissenschaft und Industrie.

Die Konferenz verabschiedete eine Erklärung zu Ethik und Datenschutz im Bereich der Künstlichen Intelligenz und darüber hinaus Entschließungen über E-Learning-Plattformen, zur Zusammenarbeit von Daten- und Verbraucherschutzbehörden sowie zur Zukunft der Internationalen Datenschutzkonferenz.

Ausgewählte Dokumente der Konferenz sind auf der Homepage des Landesbeauftragten unter dem Menüpunkt Konferenzen – Internationale Datenschutzkonferenz veröffentlicht.

5 Technik und Organisation

5.1 Das neue Landesnetz ITN-XT – Sachstand

Der Landesbeauftragte hat in seinem XIII./XIV. Tätigkeitsbericht (Nr. 4.2) über dieses Vorhaben für ein modernes, leistungsfähiges Sprach- und Datennetz ausführlich berichtet. Nach den im Jahr 2018 abgeschlossenen ca. 200 Standortbegehungen bestehen insbesondere noch hinsichtlich des erforderlichen Brandschutzes und des technischen Zustandes der Serverräume erhebliche Mängel. Mit einer neuen Projektorganisation und unter enger Einbeziehung des Landesbetriebs „Bau- und Liegenschaftsmanagement Sachsen-Anhalt“ (BLSA) sollen bis zum II. Quartal 2019 die Standortbegehungen abgeschlossen werden. Die vielen Defizite bei der lokalen LAN-Infrastruktur in den Standorten haben zu der Entscheidung geführt, die vorgesehene BSI-Grundschutzzertifizierung auf den WAN-Anschluss zu begrenzen. Allerdings setzt eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz weiterhin die Lösung der Probleme des Brandschutzes in allen Serverräumen voraus. An diesem Vorhaben hält das Ministerium der Finanzen, unter Begrenzung auf den WAN-Anschluss der Standorte, fest. Der WAN-Anschluss aller Behörden soll bis Ende des Jahres 2019 realisiert werden. Die danach notwendige LAN-Migration bzw. LAN-

Installation in den Behörden verzögert sich weiter; das BLSA wird zusätzliche Baumaßnahmen planen müssen.

Der Landesbeauftragte begrüßt die weiterhin geplante BSI-Zertifizierung des ITN-XT auf Basis der BSI-Standard-Reihe 200, auch wenn eine Begrenzung aus den genannten Gründen auf den WAN-Anschluss erfolgt. Der Beginn der Zertifizierung ist für den 30. September 2019 geplant. Die Realisierung dieses für das ganze Land so wichtigen Infrastrukturprojektes bildet für die Umsetzung auch der ambitionierten Ziele des Onlinezugangsgesetzes, ab dem Jahr 2022 bis zu 575 Verwaltungsleistungen auch online über Verwaltungsportale anzubieten, die wesentliche Grundlage.

5.2 Informationssicherheitsleitlinie – endlich verabschiedet

In seinem Beitrag Nr. 4.3 des XIII./XIV. Tätigkeitsberichts hatte der Landesbeauftragte noch über die für den Herbst 2018 avisierte Kabinettvorlage des Ministeriums der Finanzen für die überfällige Landesleitlinie zur Informationssicherheit berichtet. Die sodann mit Gemeinsamem Runderlass vom 25. September 2018 (MBl. LSA S. 443) am 4. Dezember 2018 in Kraft getretene Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalts (Informationssicherheitsleitlinie Sachsen-Anhalt – LISL LSA) steht nur für den Beginn des schwierigen ressortübergreifenden Informationssicherheitsmanagement-Prozesses. Nach vielen Jahren ist es immerhin gelungen, zumindest eine wesentliche Grundlage für ein solches ressortübergreifendes Informationssicherheitsmanagementsystem (ISMS) in Sachsen-Anhalt zu etablieren. Letztendlich setzt die Landesregierung damit einen Beschluss des IT-Planungsrates aus dem Jahre 2013 um.

Als Leitlinie richtet sich die LISL LSA auch an die mittelbare Landesverwaltung. Sie berücksichtigt die besondere Rolle der Gerichte im Bereich des Justizressorts und trägt für die Verwaltung des Landtages, den Landesrechnungshof, das Landesverfassungsgericht und den Landesbeauftragten für den Datenschutz empfehlenden Charakter.

Die Organisationsstruktur für das ressortübergreifende ISMS besteht aus:

- der Landesregierung,
- dem Beauftragten der Landesregierung des Landes Sachsen-Anhalt für Informationstechnik (CIO),
- dem Landesbeauftragten für Informationssicherheit der unmittelbaren Landesverwaltung (Chief Information Security Officer, CISO),
- dem Computer Emergency Response Team (CERT),
- den Informationssicherheitsbeauftragten der Ressorts (Ressorts-InSiBe) sowie
- den Informationssicherheitsbeauftragten der nachgeordneten Behörden, Einrichtungen und Landesbetriebe.

Die Beachtung der Sicherheitsziele der Informationssicherheit, nämlich Vertraulichkeit, Integrität und Verfügbarkeit, müssen zukünftig ein integraler Bestandteil von Planung, Konzeption und Betrieb von Verwaltungs- und Datenverarbeitungsprozessen sein. Hierbei sind insbesondere die technischen und organisatorischen Anforderungen des Datenschutzes (Art. 32 DS-GVO) zu berücksichtigen. Eine frühzeitige Einbeziehung des Landesbeauftragten durch die Landesregierung sowie auch die Beteiligung der behördlichen Datenschutzbeauftragten der Ressorts und der nachgeordneten Bereiche bei diesen Planungs- und Umsetzungsprozessen ist geboten.

Die bisherige Arbeitsgruppe „InfoSic“ bildet zukünftig das ISM-Team, das vom CISO geleitet wird und aus den Ressorts-InSiBe besteht. Der Landesbeauftragte wird bei Bedarf das ISM-Team weiter beratend unterstützen.

5.3 E-Government-Gesetz Sachsen-Anhalt – Sachstand

Der Landesbeauftragte hat sich in seinem XIII./XIV. Tätigkeitsbericht (Nr. 4.4) umfänglich und kritisch mit dem langwierigen Gesetzgebungsprozess und den Inhalten des Gesetzentwurfs der Landesregierung vom 19. September 2017 (LT-Drs. 7/1877) auch unter Einbeziehung der Vorgaben des Onlinezugangsgesetzes auseinandergesetzt.

Einhelliger Tenor der Anhörung im Landtag war das Erfordernis einer umfassenden Überarbeitung des Gesetzentwurfs. Die Koalitionsfraktionen teilen diese Bewertung und haben Änderungsbedarfe formuliert. Ein wesentlicher Aspekt betrifft die ganzheitliche Betrachtung von Landesverwaltung und Kommunalverwaltung im E-Government. Im Berichtszeitraum lag aber noch kein überarbeiteter Gesetzentwurf vor. Die Zeit drängt weiter.

Immerhin gibt es Signale, dass das Ministerium der Finanzen an einer Novellierung der alten Strategie „Sachsen-Anhalt Digital 2020“ aus dem Jahre 2012 arbeitet. Eine moderne E-Government-Strategie bildet die Voraussetzung für eine zukunftsfähige Verwaltung. Darauf hat der Landesbeauftragte auch im Digitalisierungsbeirat, der die Digitale Agenda des Landes begleitet, hingewiesen.

5.4 IT-Planungsrat – Onlinezugangsgesetz und Portalverbund

Der Landesbeauftragte informierte in seinem XIII./XIV. Tätigkeitsbericht (Nr. 4.5) über die zukünftige neue Organisationsstruktur des IT-Planungsrats (IT-PLR). Die entsprechenden Rahmenbedingungen sollen mit FITKO (Föderale IT-Kooperation) in Form einer Anstalt des öffentlichen Rechts (AöR) in gemeinsamer Trägerschaft aller Länder und des Bundes geschaffen werden. Der Aufbaustab FITKO im Hessischen Ministerium der Finanzen hat seinen Sitz in Frankfurt am Main. Die FITKO bündelt die bisherigen Geschäfts- und Koordinierungsstellen des IT-PLR und soll die Handlungs- und die politisch-strategische Steuerungsfähigkeit des IT-PLR stärken. Ein entsprechendes Umsetzungskonzept zur Ausgestaltung dieser AöR wurde vom IT-PLR und den Staats- und Senatskanzleien der Länder bereits im September 2017 bestätigt. Die Umsetzung dieser neuen Organisationsstruktur erfolgt durch die Änderung des IT-Staatsvertrages mit Bildung dieser AöR zum 1. Januar 2020.

Mit dem im August 2017 in Kraft getretenen Onlinezugangsgesetz (OZG) sind Bund, Länder und Kommunen verpflichtet, bis zum Ende des Jahres 2022 ihre Verwaltungsleistungen in einem Verbund ihrer Verwaltungsportale auch *online* anzubieten. Die Umsetzung der Anforderungen aus dem OZG erfolgt mit zwei Koordinierungsprojekten des IT-PLR gemeinsam von Bund und Ländern: dem Digitalisierungsprogramm und dem Portalverbund. Hierbei sind die Kommunen von den Ländern verbindlich einzubeziehen. Die Koordinierung der OZG-Umsetzung erfolgt auf Beschluss des IT-PLR gemeinsam durch das Bundesministerium des Innern, für Bau und Heimat und den Aufbaustab FITKO.

Im Sinne einer föderalen Zusammenarbeit werden im Rahmen des Digitalisierungsprogramms 14 Themenfelder arbeitsteilig von Bund, Ländern und Kommunen bearbeitet. Für jedes Themenfeld übernimmt eine Kooperation aus einem Bundesministerium und einem oder mehreren Ländern die gemeinsame Federführung. Für das Themenfeld „Bildung“ hat das Land Sachsen-Anhalt die Federführung übernommen. Ziel ist es generell, nutzerfreundliche digitale Leistungen anzubieten, die dann durch andere Länder und Kommunen nachgenutzt werden können.

Der OZG-Umsetzungskatalog stellt gegenwärtig 575 Verwaltungsleistungen zusammen, für die digitale Lösungen umgesetzt werden müssen. Die darin beschriebenen Leistungen sind nicht nach den Zuständigkeiten der Verwaltung sortiert und gruppiert, sondern aus *Nutzersicht*, also der Sicht von Bürgerinnen und Bürgern und Unternehmen, strukturiert. Sie sind in Lebens- und Geschäftslagen gebündelt, die sich an den wirklichen Anliegen und dem Lebensalltag der Nutzer orientieren.

Der *Portalverbund* umfasst zum einen das neue Verwaltungsportal des Bundes, mit Zugang zu allen Leistungen von Bundesbehörden, und zum anderen auch die einfache und schnelle Abrufbarkeit der Verwaltungsleistungen der Länder und Kommunen. Mittels des Portalverbunds werden die Verwaltungsportale des Bundes, der Länder *und* der Kommunen technisch verknüpft. Dadurch soll ein einheitlicher Zugang zu allen Online-Angeboten der Verwaltung ermöglicht werden. Für die Authentifizierung der Nutzer für diese digitalen Verwaltungsleistungen werden Nutzerkonten für Bürger und Unternehmen im Portalverbund bereitgestellt.

Dataport als zentraler IT-Dienstleister für sechs Trägerländer, darunter auch Sachsen-Anhalt, bietet gerade hinsichtlich der technischen Umsetzung des Portalverbundes eine vielversprechende Lösung mit der sog. *Online-Service-Infrastruktur* (OSI) als Plattform für alle Onlinedienste an. Sie umfasst alle Bausteine zur Umsetzung des OZG (Verwaltungsportale, Nutzerkonto, Basisdienste, Fachverfahren). Der Landesbeauftragte wurde im Rahmen des alljährlichen Erfahrungsaustausches zwischen dem Dataport-Vorstand und den Datenschutzbeauftragten der Trägerländer über das Konzept informiert.

Das Ministerium der Finanzen sollte diese technischen Voraussetzungen, die Dataport mit OSI zur Verfügung stellt und dem Land Sachsen-Anhalt bereits vorgestellt hat, bei der zurzeit in Überarbeitung befindlichen E-Government-Strategie des Landes berücksichtigen (s. Nr. 5.3).

5.5 Transportverschlüsselung für E-Mails in der Landesverwaltung

Im Anschluss an die Ausführungen im XIII./XIV. Tätigkeitsbericht (Nrn. 4.10, 4.11) konnte der Landesbeauftragte feststellen, dass die Landes-E-Mail-Server auf das Transportverschlüsselungsprotokoll TLS (Transport Layer Security) in der Version 1.2, mit Abwärtskompatibilität bis zur Protokollversion 1.0, umgestellt worden sind. Dieser Umstand ist aus datenschutzrechtlicher Sicht sehr zu begrüßen, wenn auch darauf hingewiesen werden muss, dass zum aktuellen Zeitpunkt nicht alle verwendeten Algorithmen dem Stand der Technik entsprechen. So wird der Hashalgorithmus SHA-1 vom BSI als angreifbar und unsicher eingestuft und die Nutzung der Nachfolger SHA-256 und SHA-512 empfohlen. Es sollte weiter das langfristige Ziel verfolgt werden, die Transportverschlüsselung zu stärken, indem neueste Algorithmen in Kombination mit der sicheren Mail-Server-Authentifizierung DANE (DNS-based Au-

thentication of Named Entities) verwendet werden. Ein Umstieg auf die TLS-Version 1.3 erleichtert die Erreichung dieses Ziels.

Die Ressorts der Landesverwaltung müssen nun ihrerseits sicherstellen, dass auch ihre E-Mail-Server auf das TLS-Protokoll umgestellt werden. Dabei ist zu beachten, dass die STARTTLS-Konfiguration der Landes-E-Mail-Server weiterhin den unverschlüsselten E-Mail-Verkehr bei Servern erlaubt, die kein TLS unterstützen. Davon ist datenschutzrechtlich jedoch dringend abzuraten.

5.6 Microsoft Cloud-Dienste – Sachstand

Im XIII./XIV. Tätigkeitsbericht (Nr. 4.12) informierte der Landesbeauftragte über die seit 2015 bestehende „Microsoft Cloud Deutschland“ (MCD). Diese sollte Bedenken bezüglich der Speicherung von Daten in Clouds außerhalb der EU und möglicher Zugriffe Dritter auf diese Daten ausräumen, indem die Rechenzentren in Deutschland betrieben werden und die Administration via Datentreuhänder T-Systems International GmbH derart erfolgt, dass der Datentreuhänder datenschutzrechtlich unzulässige Zugriffe Dritter – wie etwa durch US-Geheimdienste – auf die Kundendaten verhindert.

Der Landesbeauftragte ist Mitglied in der Ad-Hoc-Arbeitsgruppe „Microsoft Cloud Deutschland“ und auch im Unterarbeitskreis „Office 365“ des Arbeitskreises Verwaltungsmodernisierung der DSK. In diesen wurden Datenschutz-Aspekte der MCD und einzelner Cloud-Dienste wie Microsoft Office 365 erörtert und direkt mit Vertretern von Microsoft beraten.

Seit dem 31. August 2018 werden keine neuen Kunden und Dienste mehr für die MCD zugelassen, das Treuhändermodell wird Neukunden nicht mehr angeboten. Microsoft plant, das zu wenig nachgefragte Cloud-Angebot der MCD an das umfangreichere, weltweite Cloud-Angebot anzupassen. Bestandskunden erhalten nur noch operationelle Verbesserungen und Sicherheitspatches. Der Konzern wird bestehende vertragliche Verpflichtungen einhalten, auch das Verlängerungsrecht der Kunden soll weiterhin bestehen. Langfristig sollen diese zu einem Wechsel in die normale Microsoft Cloud bewegt werden. Die Einstellung des Produkts würde eine Vorlaufzeit von 12 Monaten haben.

Es sind neue Microsoft-Rechenzentren-Regionen in Deutschland – ab 2019/2020 in Berlin und Frankfurt – geplant. Microsofts Cloud-Rechenzentren sollen, schon aufgrund von Latenzzeiten, in Kundennähe betrieben werden. Der Kunde soll den Standort selbst wählen können. Microsoft bekennt sich des Weiteren zur Einhaltung der DS-GVO für die Cloud-Dienste.

Inwieweit die Anforderungen des Art. 28 DS-GVO an Auftragsverarbeiter bei Microsofts Cloud-Diensten eingehalten werden, war und ist eine zentrale Frage. In den Diskussionen einer Arbeitsgruppe der Datenschutzaufsichtsbehörden mit Microsoft ging es unter anderem um Datenübermittlungen in Drittländer oder Zugriffe durch außereuropäischen Kundensupport. Wichtig ist aus Sicht der Aufsichtsbehörden, dass der Auftraggeber als Kunde „Herr“ des Verfahrens bleibt und Datenzugriffe und -übertragungen nur auf Weisung des Kunden erfolgen. Microsoft verwies einstweilen auf seine umfangreichen Vertragsgestaltungen. Die rechtliche Bewertung von Cloud-Produkten wie Microsoft Office 365 ist noch nicht abgeschlossen.

6 Telekommunikation und Medien

6.1 E-Privacy-Verordnung – Positionsbestimmung zum Telemediengesetz

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) sollte ursprünglich zeitgleich mit der DS-GVO in Kraft treten und dabei die bislang geltende E-Privacy-Richtlinie (Richtlinie 2002/58/EG), ergänzt durch die sogenannte Cookie-Richtlinie (Richtlinie 2009/136/EG), ablösen. Allerdings verzögert sich das europäische Gesetzgebungsverfahren erheblich, sodass ein Termin für das Inkrafttreten momentan nicht absehbar ist.

Aus diesem Grund haben sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in einer vorläufigen Positionsbestimmung vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“ zu der Frage geäußert, unter welchen Voraussetzungen Tools zur Reichweitenmessung und zum Tracking datenschutzkonform eingesetzt werden dürfen. Die Grundlinie der Auffassung der Datenschutzaufsichtsbehörden besteht darin, dass die bisherige E-Privacy-Richtlinie nur unzureichend im nationalen Recht umgesetzt worden und jedenfalls in der Übergangsphase bis zum Erlass einer E-Privacy-Verordnung die Vorranganwendung der DS-GVO zu beachten ist.

Im Rahmen einer Konsultation hatten Wirtschaftsverbände und Interessenvertretungen Gelegenheit, zur Umsetzung der Positionsbestimmung Stellung zu nehmen.

Ausgehend von den im Rahmen der Konsultation genannten Aspekten erarbeitet die DSK eine Ergänzung der Positionsbestimmung. Diese soll insbesondere Konkretisierungen und Hinweise zur Interessenabwägung beim Einsatz von Tracking-Tools enthalten.

6.2 Verantwortlichkeit für Fanpages bei Facebook

Das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (C-210/16) hat die langjährige Rechtsauffassung der Datenschutzaufsichtsbehörden bestätigt, dass auch den Betreibern einer Facebook-Fanpage eine Verantwortung für die Verarbeitung der personenbezogenen Daten der Facebook-Nutzer zukommt (XIII./XIV. Tätigkeitsbericht, Nr. 5.6.1, vgl. auch Nr. 6.5).

Durch jede neue Facebook-Fanpage werden sogenannte Insights-Daten generiert. Diese statistischen Daten werden durch Auswertung personenbezogener Daten der Nutzer dieser Fanpage (auch bei Nichtmitgliedern von Facebook) erzeugt und dem Seitenbetreiber automatisch zur Verfügung gestellt. Außerdem kann Facebook diese Daten nutzen, um noch genauere Profile seiner Nutzer zu erstellen. Auch wenn keine personenbezogenen Daten auf einer Facebook-Fanpage veröffentlicht werden, besteht die datenschutzrechtliche Problematik in der Interaktion der Nutzer mit der Seite und deren Auswertung durch Facebook.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen und insbe-

sondere für die Fanpage-Betreiber ergeben **(Anlage 2)**. Der ergänzende Beschluss vom 5. September 2018 enthält außerdem einen Fragenkatalog, der sowohl von Facebook als auch von den Fanpage-Betreibern beantwortet werden muss **(Anlage 3)**.

Möglicherweise als Reaktion auf diesen Beschluss hat Facebook im September 2018 in seinen Geschäftsbedingungen eine ergänzende Regelung zu den Seiten-Insights veröffentlicht. Darin wird allerdings ein großer Teil der Verantwortung auf den Seitenbetreiber „abgewälzt“. Unter anderem verpflichtet diese Ergänzung den Seitenbetreiber sicherzustellen, dass er eine Rechtsgrundlage für die Verarbeitung von Insights-Daten gemäß DS-GVO hat, den Verantwortlichen für die Verarbeitung der Seite benennt und jedwede sonstigen geltenden rechtlichen Pflichten erfüllt hat. Außerdem wird festgelegt, dass jedweder Anspruch, Klagegegenstand oder Streitfall, der sich aus dieser Seiten-Insights-Ergänzung ergibt oder damit in Verbindung steht, ausschließlich von den Gerichten in Irland zu klären ist, sich der Seitenbetreiber unwiderruflich der Rechtsprechung der irischen Gerichte unterwirft und dass die Seiten-Insights-Ergänzung irischem Recht unterliegt.

Der Landesbeauftragte rät ausgehend von dieser Rechtslage nach wie vor vom Betrieb einer Facebook-Fanpage ab, da für die Zukunft nicht ausgeschlossen ist, dass gegen Fanpage-Betreiber auch aufsichtsrechtliche Maßnahmen ergriffen werden, wenn diese ihren Verpflichtungen gemäß DS-GVO – insbesondere ihren Informationspflichten – nicht in ausreichendem Umfang nachkommen.

Im Übrigen dürfte die Rechtsauffassung des EuGH zu den Facebook-Fanpages auf die Einbindung von „Gefällt-mir“-Buttons von Facebook auf Webseiten übertragbar sein; hierzu läuft noch ein Verfahren vor dem EuGH.

Des Weiteren ist bemerkenswert, dass das Bundeskartellamt am 7. Februar 2019 Facebook einen Missbrauch seiner marktbeherrschenden Stellung vorgeworfen hat, indem es nicht nur auf der eigenen Plattform Daten sammelt, sondern auch über die konzerneigenen Dienste wie WhatsApp und Instagram sowie auf Drittwebseiten und Apps mit entsprechenden Schnittstellen. Das Bundeskartellamt hat Facebook deshalb weitreichende Beschränkungen bei der Verarbeitung von Nutzerdaten auferlegt. Zukünftig dürfen Nutzerdaten, die aus verschiedenen Quellen stammen, nur noch dann dem Nutzerkonto zugeordnet werden, wenn der Nutzer darin explizit und freiwillig einwilligt. Das heißt, dass die Nutzung der Facebook-Dienste nicht von der Einwilligung des Nutzers in diese Art der Datensammlung und -zusammenführung abhängig gemacht werden darf.

6.3 Recht am eigenen Bild

Der Landesbeauftragte wurde durch Pressesprecher öffentlicher Stellen zum Recht am eigenen Bild im Zusammenhang mit der Anwendbarkeit der DS-GVO angefragt. Bisher hatte man auf eine entsprechende Anwendbarkeit der Regelungen des Kunsturhebergesetzes (KunstUrhG) gesetzt. Zunächst hat der Landesbeauftragte Zurückhaltung empfohlen. Fotos von Betroffenen sollten möglichst auf Basis der Einwilligung verwendet werden. Die Nutzung von Fotos insbesondere in digitalen Medien stellt aufgrund des vereinfachten Zugriffs und der unkontrollierbaren Vervielfältigungsmöglichkeit einen schweren Eingriff in das Betroffenenrecht dar. Grundsätzlich ist die Verwendung von Fotos zur Erfüllung von Aufgaben der öffentlichen Verwaltung nicht erforderlich, sodass schon insoweit die Zulässigkeit der Verwendung von

Fotos ohne Einwilligung fraglich ist. In der rechtlichen Beurteilung war sodann umstritten, ob das KunstUrhG nach Wirksamwerden der DS-GVO noch Geltung beanspruchen kann.

Dazu hat das Bundesministerium des Innern, für Bau und Heimat die Auffassung vertreten, dass sich das KunstUrhG auf die Regelungsbefugnis in Art. 85 Abs. 1 DS-GVO stützen könne. In einer Antwort der Bundesregierung auf eine Kleine Anfrage (BT-Drs. 19/3341, S. 8) wurde dargelegt, dass das KunstUrhG fortwirkt. Bestätigung fand dies in der Entscheidung des Oberlandesgerichts Köln vom 18. Juni 2018 (Az.: 15 W 27/18). Allerdings bezieht sich diese Auffassung vor allem auf den journalistischen Bereich.

Es ist jedenfalls davon auszugehen, dass die Wertungen aus den §§ 22, 23 KunstUrhG im Rahmen der Prüfung der Erforderlichkeit nach dem DSG LSA für öffentliche Stellen (wie auch für die Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO für nichtöffentliche Stellen) einbezogen werden können. Die DS-GVO betont in Erwägungsgrund 4, dass das Recht auf Schutz der personenbezogenen Daten im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss. Im Rahmen der Prüfung des Einzelfalles kann das legitime Interesse der öffentlichen Stelle an der Darstellung ihrer Politik oder ihres Verwaltungshandelns das Schutzinteresse des Betroffenen überwiegen, wenn die Person auf einem Bild nur als Beiwerk oder als Teilnehmer einer Veranstaltung erfasst ist und keine besonderen Gründe entgegenstehen (Kind, Intimsphäre betroffen, Diskreditierung).

Weiter erreichten den Landesbeauftragten Anfragen, die Verbote an Schulen beklagten, im Rahmen von Einschulungsveranstaltungen Fotos anzufertigen. Hierbei sind verschiedene Fallgestaltungen zu unterscheiden. Unterschiede ergeben sich schon danach, ob nur Eltern für das Familienalbum fotografieren oder ein professioneller Fotograf im Eigeninteresse oder im Auftrag der Schule tätig wird.

Grundsätzlich sind Schulleitungen befugt, im Rahmen des Hausrechts ein Fotografierverbot zu verhängen, z. B. zum Schutz der Beteiligten oder zur Vermeidung von zivilrechtlichen Auseinandersetzungen. Erfolgt kein Verbot, ist jeweils die Rechtsgrundlage für Aufnahmen zu prüfen. Wenn Eltern nur für das Familienalbum Aufnahmen machen, ergibt sich aus der DS-GVO keine Einschränkung, es greift die sog. Haushaltsausnahme (keine Geltung bei Ausübung persönlicher oder familiärer Tätigkeit, Art. 2 Abs. 2 lit. c DS-GVO).

Ist die DS-GVO anwendbar, also z. B. bei Aufnahmen durch die Schule selbst, kommt das SchulG LSA und bei Aufnahmen durch zugelassene Berufsfotografen oder auch durch Schülerinnen und Schüler untereinander im Rahmen der Nutzung des Smartphones u. a. auf dem Schulhof Art. 6 Abs. 1 lit. f DS-GVO in Betracht.

Bei der Interessenabwägung wäre dem legitimen Anliegen des Aufnehmenden (Erwerbszwecke des Fotografen oder Dokumentationsinteressen der Schule (Meinungsfreiheit, Kunstfreiheit, Berufsfreiheit)) das Schutzinteresse (besonders geschützte zur Anwesenheit verpflichtete Kinder einerseits; andererseits aber auch: nur Teilöffentlichkeit, nur Sozialsphäre betroffen, nur Teilnahme an einer Veranstaltung (Wertung des KunstUrhG)) gegenüber zu stellen. Bei entsprechenden Rahmenbedingungen (vorherige Ankündigung des Fotografierens, fotografierfreie Rückzugsräume etc.)

können Aufnahmen ggf. zulässig sein. Hierzu ist ergänzend auf die Veröffentlichung „Datenschutz an Schulen“[2] des Ministeriums für Bildung des Landes Sachsen-Anhalt hinzuweisen.

7 Öffentliche Sicherheit, Meldewesen

7.1 SOG LSA

Mit seinem XIII./XIV. Tätigkeitsbericht (Nr. 6.2) hat der Landesbeauftragte die mit der 6. und 7. Novelle vorgenommenen Änderungen des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) dargestellt und aus datenschutzrechtlicher Sicht bewertet. Das dort erwähnte „Siebente Gesetz zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt“ wurde zwischenzeitlich vom Landtag Sachsen-Anhalt beschlossen und trat am 30. Oktober 2018 in Kraft (GVBl. LSA S. 376).

Letztendlich wurde das SOG LSA durch das „Gesetz zur Polizeistrukturreform“ (GVBl. LSA 2018, S. 406) zum Jahresende nochmals geändert. Mit diesem Gesetz wurde zum 1. Januar 2019 eine neue Polizeistruktur mit vier Polizeiinspektionen, die die alten Polizeidirektionen ablösen, und einer Polizeiinspektion „Zentrale Dienste“ eingeführt.

Hinsichtlich des im XIII./XIV. Tätigkeitsbericht (Nr. 6.2) bereits dargestellten Entwurfs einer weiteren Änderung des SOG LSA mit dem „Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes“ (LT-Drs. 7/3207) wird zunächst auf die Ausführungen unter Nr. 4.1.2 verwiesen.

Eine geplante Neuregelung im SOG LSA sieht die Erfassung von DNA-Identifizierungsmustern zur Erkennung von Trugspuren auf Basis einer Einwilligung betroffener Polizeibediensteter vor (§ 23d). Das Abstellen auf die Rechtsgrundlage der Einwilligung erscheint grundsätzlich positiv, auch wenn die Gesetzesbegründung nicht im Ansatz erläutert, welche negativen Erfahrungen in Sachsen-Anhalt in den letzten Jahren die Regelung rechtfertigen könnten. Unverhältnismäßig ist jedoch die vorgesehene Regelung, wonach die DNA-Identifizierungsmuster pseudonymisiert und nicht anonymisiert gespeichert werden dürfen, um ermitteln zu können, auf welche Weise Spurenmaterial verunreinigt wurde. Der Landesbeauftragte hat in der Beratung des Ministeriums für Inneres und Sport und in seiner Stellungnahme gegenüber dem Landtag von Sachsen-Anhalt erläutert, dass es damit nicht mehr nur um die Abwehr von Beeinträchtigungen des Ermittlungsverfahrens geht, sondern auch um Erkenntnisse, die ggf. bei Überlegungen zu anschließenden Prozessoptimierungen hilfreich sein können. Allein dies vermag eine personenbeziehbare Speicherung äußerst sensibler Daten nicht zu rechtfertigen. Ein Hinterlegen in anonymisierter Form als mildestes Mittel reicht zum Schutz des Ermittlungsverfahrens aus.

[2] https://bildung.sachsen-anhalt.de/schulen/datenschutz/handreichung-datenschutz-an-schulen/

Eine weitere Regelung sieht vor, dass auf der Grundlage einer Einwilligung die im Informationssystem der Polizei des Landes Sachsen-Anhalt gespeicherten Daten oder die im polizeilichen Informationsverbund bereitstehenden Daten zum Zwecke der Durchführung einer Zuverlässigkeitsüberprüfung bei der Einstellung in den Polizeivollzugsdienst weiterverarbeitet werden können (§ 29). Hierzu verwies der Landesbeauftragte darauf, dass dies den hohen Anforderungen an die Freiwilligkeit einer Einwilligung nach der DS-GVO und der JI-Richtlinie nicht genügt. Auch wurde auf die höchstrichterliche Rechtsprechung Bezug genommen, nach der der pauschale Zugriff auf unspezifizierte und zudem oftmals nicht hinreichend belastbare Daten aus Informationssystemen der Polizei und Ermittlungsbehörden mit grundrechtlichen Vorgaben der Erforderlichkeit und Verhältnismäßigkeit nicht vereinbar ist.

Ohnehin ist das Ansinnen, für Einstellungen in den Polizeivollzugsdienst auf Daten der Informationssysteme zuzugreifen, nicht mit Bundesrecht vereinbar. Danach stehen für Einstellungsverfahren, auch im öffentlichen Dienst, grundsätzlich Führungszeugnisse zur Verfügung. Verurteilungen, Schuldsprüche oder Verwarnungen mit Strafvorbehalt und natürlich erst Recht bloße Informationen, die nicht nach § 41 BZRG aufgenommen werden, dürfen dem Betroffenen im Rechtsverkehr gerade nicht entgegengehalten werden. § 43 BZRG regelt abschließend, wofür welche Informationen verwendet werden dürfen. Einstellungen in den Polizeivollzugsdienst sind bewusst nicht enthalten. Abfragen hierfür würden daher eine Umgehung der §§ 41, 43 BZRG darstellen und der Unschuldsvermutung (Art. 6 Abs. 2 EMRK) und dem Rechtsstaatsgebot widersprechen.

Bei Redaktionsschluss dauerten die Beratungen in den Landtagsausschüssen noch an.

7.2 Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung

Der Landesbeauftragte hat bereits in seinem XIII./XIV. Tätigkeitsbericht (Nr. 6.6) zum Gemeinsamen Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung (GKDZ) berichtet. Im aktuellen Berichtszeitraum wurde dem Landesbeauftragten zum Planungsstand mitgeteilt, dass das GKDZ personell und finanziell handlungsfähig sei.

Für alle Teilnehmerländer (Berlin, Brandenburg, Sachsen, Sachsen-Anhalt, Thüringen) fand zu Beginn des Jahres 2019 eine Veranstaltung statt, bei der Grundzüge der technischen und organisatorischen Umsetzung der Feinplanung und erste Datenschutzanforderungen vorgestellt wurden. Die Landesbeauftragten werden weiterhin das – noch nicht im Betrieb befindliche – Vorhaben begleiten.

7.3 E-Evidence-Verordnung

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) beabsichtigt die EU-Kommission, eine Alternative zum förmlichen Rechtshilfeverfahren zu schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten zu ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitglied-

staaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Das Vorhaben stößt rechtspolitisch auf Widerstand. Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich zu diesem Verordnungsentwurf mit einer Entschließung anlässlich der 96. Konferenz im November 2018 geäußert und kritisch Stellung genommen (**Anlage 6**).

Als besonders bedenklich bewertet die Konferenz dabei, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u. a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die Konferenz hat daher an alle im Gesetzgebungsverfahren Beteiligten appelliert, dem Vorschlag für eine E-Evidence-Verordnung nicht zuzustimmen.

7.4 Veröffentlichung von Jubiläumsdaten

Den Landesbeauftragten erreichten wieder Anfragen zur Veröffentlichung von Jubiläumsdaten. Zur dieser Frage wurde bereits im XI. Tätigkeitsbericht (Nrn. 5.9.3 und 5.9.4) ausführlich Stellung genommen.

In den aktuellen Fällen sind die Betroffenen davon ausgegangen, dass aufgrund der seit Mai 2018 geltenden DS-GVO die Veröffentlichung von Jubiläumsdaten unzulässig sei. Der Landesbeauftragte hat darauf hingewiesen, dass die Veröffentlichung von Jubiläumsdaten auch unter der DS-GVO nach dem Bundesmeldegesetz (BMG) möglich ist, denn die Öffnungsklausel in Art. 6 DS-GVO erfasst nicht nur neue Gesetze, sondern auch bestehende Regelungen wie das BMG.

Aus diesem Grunde ist eine Übermittlung von Jubiläumsdaten unter den Voraussetzungen des § 50 Abs. 2 BMG zulässig. Auf die Widerspruchsmöglichkeit § 50 Abs. 5 BMG wurde hingewiesen.

8 Verfassungsschutz

Das Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) ist im Berichtszeitraum nicht geändert worden. Eine erste konkretere Änderung zeichnet sich aber bereits ab: Mit dem Entwurf eines „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“ (vgl. Nr. 4.1.2) ist auch eine Änderung des VerfSchG-LSA vorgesehen. Dabei geht es um die Anwendung datenschutzrechtlicher Vorschriften auf den Verfassungsschutz. Das Recht des Verfassungsschutzes fällt weder in den datenschutzrechtlichen Anwendungsbereich der DS-GVO noch der JI-Richtlinie.

Das VerfschG-LSA hat aber in der Vergangenheit und auch heute noch auf die Regelungen des DSG LSA abgestellt und keine eigenen datenschutzrechtlichen Regelungen getroffen. Die bereits mit Blick auf diese europarechtlichen Regelungen (DS-GVO, JI-Richtlinie) im DSG LSA vorgenommenen Änderungen haben Einfluss auf den Umgang mit personenbezogenen Daten durch die Verfassungsschutzbehörde. Bestimmte Regelungen sind dabei für die Arbeit der Verfassungsschutzbehörde nicht gewollt, weshalb mit dem vorstehend bezeichneten Gesetzentwurf in Bezug auf das VerfSchG-LSA sichergestellt werden soll, dass nach wie vor die „alten“ Regelungen des DSG LSA – mithin die, die vor 2018 gegolten haben – für die Verfassungsschutzbehörde weiterhin den datenschutzrechtlichen Rahmen ihrer Tätigkeit bieten.

Darüber hinaus steht eine grundlegende Novellierung des VerfSchG-LSA mit zusätzlichen Aufgaben und Befugnissen für die Verfassungsschutzbehörde bevor. Der Landesbeauftragte wird darauf Wert legen, dass dabei verfassungsrechtliche Maßstäbe gewahrt bleiben und auch datenschutzrechtliche Kontrollmöglichkeiten erweitert werden.

9 Rechtspflege und Justizvollzug

9.1 Datenschutz im Justizvollzug

Für den Bereich des Justizvollzuges (insbesondere Strafhaft, auch Untersuchungshaft und Jugendstrafhaft, zusätzlich Jugendarrest) gilt nicht die DS-GVO, sondern 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“ (sog. JI-Richtlinie). Sie trat am 5. Mai 2016 in Kraft und war bis zum 6. Mai 2018 in nationales Recht umzusetzen.

Der Landesbeauftragte hat bereits in seinem XIII./XIV. Tätigkeitsbericht (Nr. 3.1.2) berichtet, dass das Ministerium für Justiz und Gleichstellung trotz des Fristablaufs der Umsetzungsvorgabe bis 6. Mai 2018 keinen entsprechenden Gesetzentwurf vorgelegt hatte, und darauf hingewiesen, dass eine zeitnahe europarechtskonforme Umsetzung der Richtlinie im Justizvollzug dringend geboten sei.

Im Oktober 2018 erfolgte dann eine Anhörung durch das Ministerium für Justiz und Gleichstellung zum „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung der Datenschutzvorschriften im Bereich des Justizvollzuges von Sachsen-Anhalt (Justizvollzugsdatenschutzumsetzungsgesetz Sachsen-Anhalt)“. Der Landesbeauftragte, der im Vorfeld bei der Erstellung des Referentenentwurfs nicht beteiligt worden war, hält große Teile des Entwurfs für problematisch. Zu nennen sind hier die

- unübersichtliche Gesetzessystematik,
- Verwendung neuer Begriffe, die die Richtlinie nicht vorgesehen hat,
- europarechtswidrige Einschränkung bereits bestehender Kontrollkompetenzen des Landesbeauftragten,

- geplante Erleichterung des Einsatzes privater Dienstleister für hoheitliche Maßnahmen,
- Einräumung präventiv-polizeilicher Befugnisse zur Abwehr drohender Gefahren an eine Strafvollstreckungsbehörde, d. h. von Befugnissen, die nicht einmal die Polizei besitzt,
- weitreichenden Regelungen zur Überprüfung anstaltsfremder Personen, insbesondere von Besuchern, durch den Verfassungsschutz.

Das Ministerium für Justiz und Gleichstellung bezieht in den Gesetzentwurf auch den Regelungsbereich des Sicherungsverwahrungsvollzuges ein, obwohl dieser ein aliud ist, also etwas ganz anderes als die Strafvollstreckung. Insofern dürfen nicht inhaltsgleiche Regelungen der Datenverarbeitung im Justizvollzug anwendbar sein.

Der Landesbeauftragte hat insgesamt eine umfassende Überarbeitung des Gesetzentwurfs empfohlen. Die Landesregierung ist seinem Rat jedoch nicht gefolgt, sondern hat den Gesetzentwurf im Januar 2019 nahezu unverändert in den Landtag eingebracht (LT-Drs. 7/3858). Die Beratungen im Parlament sind abzuwarten.

9.2 Anwendung der Datenschutz-Grundverordnung bei den Gerichten

Im Geschäftsbereich des Ministeriums für Justiz und Gleichstellung stellte sich die Frage, welche datenschutzrechtlichen Vorschriften für die Gerichte seit der Anwendbarkeit der DS-GVO ab Mai 2018 gelten. Der Landesbeauftragte erläuterte im Rahmen von zwei Informationsveranstaltungen, dass zunächst zwischen den allgemeinen Verwaltungsangelegenheiten der Gerichte und den justiziellen Tätigkeiten zu unterscheiden sei.

Hinsichtlich der Verwaltungsangelegenheiten gilt für alle Gerichte die gleiche Rechtsgrundlage, nämlich die DS-GVO. Hingegen ist das BDSG in diesem Bereich derzeit nicht anwendbar, da im Landesrecht mit § 22 Abs. 1 Satz 2 DSG LSA eine landesrechtliche Regelung existiert (§ 1 Abs. 1 Nr. 2 BDSG). Die Landesregierung beabsichtigt, im Rahmen der Novellierung des Datenschutzrechts in Sachsen-Anhalt im DSAG LSA (s. oben, Nr. 4.1.1) eine entsprechende Regelung für die Justiz aufzunehmen. Aus diesem Grund wird voraussichtlich auch zukünftig das BDSG im Bereich der Verwaltungsangelegenheiten keine Anwendung finden. Zu beachten ist, dass die Gerichte, soweit sie in Verwaltungsangelegenheiten tätig werden, weiterhin der Kontrolle durch den Landesbeauftragten unterliegen.

Bei den justiziellen Tätigkeiten ist zu unterscheiden, ob es sich um allgemeine Gerichte oder Strafgerichte handelt. Bei den allgemeinen Gerichten gilt die DS-GVO, jedoch besteht für den Landesbeauftragten keine Aufsichtszuständigkeit (Art. 55 Abs. 3 DS-GVO). Auch in diesem Bereich gilt das BDSG aktuell nicht, da das DSG LSA eine landesrechtliche Regelung enthält. Jedoch könnte zukünftig das BDSG gelten, da das DSAG LSA voraussichtlich nur für Verwaltungstätigkeiten der Gerichte gelten wird. Im Bereich der justiziellen Tätigkeiten der Gerichte ist zu beachten, dass bereichsspezifische Regelungen vorrangig sind (z. B. ZPO).

Besonderheiten gegenüber den allgemeinen Gerichten sind bei den Strafgerichten zu berücksichtigen. Für sie gilt die DS-GVO nicht, da die sog. JI-Richtlinie hier Anwendung findet. Aktuell gilt das BDSG nicht für die Strafgerichte, da eine Regelung im Landesrecht existiert. Auch zukünftig wird in diesem Bereich das BDSG voraus-

sichtlich keine Anwendung finden, da im Rahmen der Umsetzung der JI-Richtlinie in Landesrecht im DSUG LSA (s. Nr. 4.1.2) eine entsprechende Regelung enthalten sein wird. Auch im Bereich der Strafgerichte ist zu beachten, dass bereichsspezifische Regelungen vorrangig sind (z. B. StPO). Der Landesbeauftragte ist auch im Bereich der justiziellen Tätigkeiten der Strafgerichte keine Aufsichtsbehörde (Art. 45 Abs. 2 JI-Richtlinie).

9.3 Elektronischer Rechtsverkehr in der Justiz – Sachstand

Der Landesbeauftragte hatte zuletzt in seinem XIII./XIV. Tätigkeitsbericht (Nr. 8.2) über die Einführung des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akte (eAkte) im Land informiert. Im Berichtszeitraum fanden zwei Sitzungen des Projektlenkungsausschusses des Ministeriums für Justiz und Gleichstellung statt, an dem der Landesbeauftragte als Gast teilgenommen hat.

Beim Betrieb des ERV über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) selbst war seit 1. Januar 2018 keine signifikante Steigerung der Eingangszahlen bei den zentralen Eingangsstellen der Gerichte festzustellen. Grund dafür waren die technischen Probleme bei der Einführung des „besonderen elektronischen Anwaltspostfachs“ (beA). Die Freigabe der beA-Postfächer erfolgte erst wieder zum September 2018.

Daneben sollte für alle anderen Behörden des Landes – um auch für die übrigen Behörden außerhalb der Justiz den ERV mit der Justiz zu gewährleisten – ebenfalls ein elektronisches Postfach eingerichtet werden, das „besondere elektronische Behördenpostfach“ (beBPo). Gemäß Kabinettbeschluss wurde die Aufgabe der beBPo-Prüfstelle dem zentralen IT-Dienstleister Dataport übertragen. Die Authentifizierung der Behördenpostfächer steht noch aus, denn der erforderliche Durchführungserlass des Ministeriums liegt noch nicht vor. Auch hier drängt, ähnlich wie beim E-Government-Gesetz des Landes (s. Nr. 5.3), die Zeit (vgl. auch LT-Drs. 7/3818).

10 Forschung, Hochschulen und Schulen

10.1 Forschung

10.1.1 Forschungsprojekte

Im Berichtszeitraum wurde der Landesbeauftragte bei 6 neuen Forschungsprojekten beteiligt. Überdies erfolgte bei einigen Projekten im Bildungsbereich mit vorgesehenen Erhebungswellen eine erneute datenschutzrechtliche Begleitung (z. B. die Projekte „Gesundheitsverhalten und Unfallgeschehen im Schulalter“, „INSIDE“ (Inklusion in der Sekundarstufe I in Deutschland) und „Bildungsstandards“).

10.1.2 Reichweite der Einwilligung (Broad Consent)

Medizinische Forschung liegt im gesellschaftlichen Interesse und wird umfangreich gefördert, wie beispielsweise die Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung zeigt. Laut Koalitionsvertrag auf Bundesebene will Deutschland Vorreiter bei der Einführung digitaler Innovationen im Gesundheitswesen sein, wofür vor allem Daten gebraucht werden. Forscher, Forschungseinrichtun-

gen und Fachgesellschaften betonen gerade in Zeiten der Digitalisierung, Vernetzung und Einbeziehung Künstlicher Intelligenz immer wieder den Bedarf an einem umfassenden Datenbestand, der langfristig und möglichst ohne einschränkende Zweckbestimmung zur Verfügung steht. Grundsätzlich ist die Datenverarbeitung zu Forschungszwecken in einzelnen Fachgesetzen und auch in der DS-GVO privilegiert. Der Zugang für Forscher zu Datenbeständen bedarf aber nach derzeitiger Rechtslage weiterhin zumeist der Einwilligung der Betroffenen.

Vor diesem Hintergrund stellt sich die Frage, wie der Erwägungsgrund (ErwGr) 33 der DS-GVO zu interpretieren ist, der davon ausgeht, dass der Zweck der Forschung zum Zeitpunkt der Erhebung oft noch nicht vollständig angegeben werden kann und deshalb eine Einwilligung für „bestimmte Bereiche wissenschaftlicher Forschung“ unter Einhaltung der anerkannten ethischen Standards akzeptiert. Die informierte, konkrete Einwilligung (informed consent), die der ErwGr 32 grundsätzlich vorgibt, könnte zu einer breiten Einwilligung mit gewissen Einschränkungen der Zweckbestimmung (broad consent) werden. Dabei bestehen aber Zweifel, denn die konkrete Zweckbindung (festgelegte und eindeutige Zwecke) ist ein maßgeblicher Grundsatz der Datenverarbeitung nach Art. 5 Abs. 1 lit. b DS-GVO.

Die Datenschutzkonferenz hat sich daher mit dem Thema befasst und den Arbeitskreis Wissenschaft und Forschung und den Arbeitskreis Gesundheit und Soziales beauftragt, eine Positionierung zum Begriff der „bestimmten Bereiche wissenschaftlicher Forschung“ zu erarbeiten. Hierzu fanden durch den Arbeitskreis Wissenschaft und Forschung mit den Interessenvertretern und Fachgesellschaften Erörterungen statt. Im Hinblick auf den nachvollziehbaren Bedarf an einem breiten Zugang zu Forschungsdaten werden Kompensationen zur relativen Unbestimmtheit der Zweckbestimmung erwogen, wie beispielsweise die erhöhte Transparenz (Verfolgung der Entwicklung des Projekts im Internet), die weitere Einbeziehung eines Ethikvotums in nicht vorhergesehene Verwendungen oder die wiederholte Kontaktierung des Einwilligenden. Formulierungen wie etwa die Einwilligung in „medizinische Forschung“ oder „Bildungsforschung“ erscheinen aber zu unbestimmt. ErwGr 33 spricht von „bestimmten Bereichen wissenschaftlicher Forschung“. Auch die Artikel-29-Datenschutzgruppe hatte in ihren „Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679“ festgehalten, dass die DS-GVO nicht so ausgelegt werden kann, dass Verantwortliche den Grundsatz der Zweckbindung umgehen können.

Die abschließende Bewertung durch die Datenschutzkonferenz steht noch aus.

10.1.3 Ortschroniken

An den Landesbeauftragten wenden sich häufig engagierte Bürgerinnen und Bürgern sowie Vereine, die eine Chronik über ihren Ort verfassen wollen. Dabei stellt sich regelmäßig die Frage, ob personenbezogene Daten in die Chronik Eingang finden dürfen. Hierzu hat der Landesbeauftragte auf die mögliche Rechtsgrundlage in Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung) hingewiesen. Im Ergebnis ist davon auszugehen, dass in der gebotenen Abwägung der Interessen der Schutz der Betroffenen dem Interesse des Chronisten oft vorgeht. Dies gilt insbesondere bei Verwendung von Fotos; auf die Wertungen des Kunsturhebergesetzes wurde hingewiesen. Generell dürfte die Einholung der Einwilligung zur Aufnahme von personenbezogenen Daten noch lebender Personen in eine Ortschronik notwendig sein. Der Landesbeauftragte hat umfängliche Hinweise auf seiner Homepage veröffentlicht.

10.2 Schulwesen

10.2.1 Handreichung „Datenschutz an Schulen“

Wie die ungenügende Umsetzung der Verpflichtung, an Schulen Datenschutzbeauftragte zu benennen, in der Vergangenheit gezeigt hat (vgl. XIII./XIV. Tätigkeitsbericht, Nr. 9.2.1), ist es notwendig, Schulen bei der korrekten Umsetzung datenschutzrechtlicher Verpflichtungen zu unterstützen. Dies gilt insbesondere vor dem Hintergrund der Neuerungen durch die DS-GVO und der entsprechenden Anpassung im Landesschulgesetz (XIII./XIV. Tätigkeitsbericht, Nr. 9.2.2). Hierzu hat das Ministerium für Bildung des Landes Sachsen-Anhalt die umfangreiche Handreichung „Datenschutz an Schulen“ nebst einigen Anlagen herausgegeben[3]. Diese enthält Erläuterungen zu einzelnen materiellen Verpflichtungen, z. B. zum Verzeichnis der Verarbeitungstätigkeiten, zum Einsatz digitaler Geräte, zu technischen und organisatorischen Maßnahmen und zu schulspezifischen Fragestellungen (Noten- und Klassenbücher, Förderverein, Elternvertretungen).

Der Landesbeauftragte wurde durch das Ministerium bei der Erstellung beteiligt und konnte erste Hinweise geben. Zum Konzept der Handreichung gehört, dass die Dokumente kontinuierlich ergänzt und aktualisiert werden. Dazu werden weitere Vorschläge zur Optimierung und Ergänzung beim Landesbeauftragten erarbeitet.

Im Übrigen steht die Schuldatenverordnung mit Details zu den Datenverarbeitungsvorschriften des Landesschulgesetzes (§§ 84a-e) weiterhin aus. Auch fehlt noch eine Verordnung zur Gestaltung des Bildungsmanagementsystems (§ 84f).

10.2.2 Digitalpakt Schule

Seit vielen Jahren steht der Digitalpakt Schule auf der politischen Agenda, der die Technikausstattung der Schulen als Teil digitaler Bildung fördern soll. Finanzmittel in Höhe von fünf Milliarden Euro stehen im Raum, die innerhalb von fünf Jahren seitens des Bundes den Ländern zur Verfügung gestellt werden sollen. Damit könnte auch im Land Sachsen-Anhalt eine zukunftsträchtige technische Infrastruktur für Schulen bereitgestellt werden (Anbindung ans Glasfasernetz, Schulhausvernetzung, digitale Tafeln mit Internetanschluss). Im Hinblick auf die Länderzuständigkeit für die Bildung unter Ausschluss der Einwirkung des Bundes („Kooperationsverbot“) war zunächst eine Vereinbarung auf Basis des Art. 91c GG angedacht. Dies verzögerte sich, denn der Bund bestand auf einer Änderung des Art. 104c GG, der die Mitfinanzierung der Schulen durch den Bund ermöglichen sollte.

Der Bundestag hat eine entsprechende Änderung des Art. 104c GG beschlossen, wonach der Bund den Ländern zur Sicherstellung der Qualität und der Leistungsfähigkeit des Bildungswesens Finanzhilfen gewähren kann (BT-Drs. 19/3440 und 19/6144). Die Bundesländer lehnten jedoch die Grundgesetzänderung ab, da sie u. a. ihre Bildungshoheit bedroht sahen. Kritisch aus ihrer Sicht war vor allem die Pflicht zur Ko-Finanzierung bei allen Bund-Länder-Projekten. Der Bundesrat beschloss am 14. Dezember 2018, den Vermittlungsausschuss anzurufen, mit dem Ziel einer grundlegenden Überarbeitung (BR-Drs. 622/18 (Beschluss)).

---

[3] https://bildung.sachsen-anhalt.de/schulen/datenschutz/handreichung-datenschutz-an-schulen/

Mit einer Verständigung im Vermittlungsausschuss dürfte es noch im ersten Quartal 2019 zu einer Verwaltungsvereinbarung zwischen Bund und Ländern kommen, an die sich die Mittelverteilung anschließen wird. Auf Sachsen-Anhalt sollen bis 2022 insgesamt ca. 130 Millionen Euro für eine Verbesserung der technischen Infrastruktur der Schulen entfallen. Dafür ist ein neues Landeskonzept bzw. die Überarbeitung der Rahmenempfehlung zur Förderung der IT-Ausstattung der Schulen erforderlich. Die Förderung muss aber die Vorlage von Medienbildungskonzepten voraussetzen, da Technikausstattung allein noch keine Medienbildung bewirkt.

Parallel geht es um die verstärkte Verankerung von Medienbildung und Medienpädagogik in der Lehrerausbildung und Lehrerfortbildung sowie in den Lehrplänen. Für den Einsatz digitaler Lernwerkzeuge im Unterricht wird im Übrigen eine Ergänzung des Landesschulgesetzes notwendig werden.

10.2.3 Medienkompetenz

Aspekte und Entwicklungen des Datenschutzes durch Bildung, der Stärkung des Datenschutzbewusstseins und der Vermittlung von Medienkompetenz hat der Landesbeauftragte zuletzt im XIII./XIV. Tätigkeitsbericht (Nr. 9.2.4) dargestellt und kommentiert.

Im zweiten Halbjahr 2018 hat die Landesarbeitsgemeinschaft „Medienbildung / Medienkompetenz“ unter Leitung des Bildungsministeriums nicht mehr getagt. Das Bildungsministerium Sachsen-Anhalt hat immerhin im September 2018 die Endfassung des Landeskonzepts „Bildung in der digitalen Welt durch den Einsatz digitaler Medien und Werkzeuge an den Schulen des Landes Sachsen-Anhalt“ veröffentlicht.

Der Landesbeauftragte wirkte maßgeblich an der fünften Fachkonferenz des Netzwerks Medienkompetenz mit, die sich mit den Veränderungen in der Lebenswelt von Jugendlichen und deren Kommunikationsverhalten befasste und Herausforderungen für die Medienpädagogik im Hinblick auf die Nutzung digitaler Medien diskutierte.

In der Kooperation der Gremien der Kultusministerkonferenz mit dem zuständigen Arbeitskreis der DSK zu rechtlichen und technischen Umsetzungsthemen der Strategie von 2016 geht es zunächst um Überlegungen im Hinblick auf die Verankerung des Datenschutzes in Rahmenstandards für die Lehrerbildung.

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

Durch die stetige Digitalisierung der Gesellschaft (vgl. auch die Umsetzungsstrategie der Bundesregierung für Handlungsfelder des Digitalen Wandels, BT-Drs. 19/5810) und allgegenwärtige Gefährdungen und Beeinträchtigungen der Informationssicherheit wird aber auch hierfür ein weiterer Personalaufwuchs beim Landesbeauftragten immer dringlicher.

11 Gesundheits- und Sozialwesen

11.1 Gesundheitswesen

11.1.1 Digitalisierungsprojekte

Der Einsatz digitaler Technologien gewinnt auch im Gesundheitswesen immer mehr an Bedeutung. Dadurch wächst nicht nur der Umfang an Daten, sondern auch das Potential an Zugriffen durch Dritte. Die Frage der Datensicherheit spielt damit eine entscheidende Rolle.

Ein großer Bereich der Digitalisierung im Gesundheitswesen ist die Telemedizin (s. hierzu auch XIII./XIV. Tätigkeitsbericht Nr. 10.1.4). So hat die Kammerversammlung der Ärztekammer Sachsen-Anhalt am 3. November 2018 eine Änderung der Berufsordnung für Ärzte beschlossen. Diese erweitert die Fernbehandlungsmöglichkeiten. Bisher war eine Fernbehandlung, z. B. durch Videokonferenz, nur ergänzend zur direkten persönlichen Behandlung eines Patienten möglich. Nunmehr ist sie auch bei einem unbekannten Patienten zulässig, wenn dies ärztlich vertretbar ist und die erforderliche ärztliche Sorgfalt gewahrt wird.

Ein weiteres Arbeitsfeld sind elektronische Patientenakten. Krankenkassen und Ärzteverbände haben sich im Oktober 2018 mit dem Bundesgesundheitsministerium auf ein Grobkonzept zur Schaffung digitaler Standards geeinigt. Die elektronische Patientenakte soll für alle gesetzlich Versicherten bis spätestens 2021 zur Verfügung stehen.

Ein dazugehöriges Digitalisierungsprojekt ist eine App namens „Vivy“. Versicherte können über diese App Arztbriefe, Befunde, Laborwerte, Medikationspläne, Notfalldaten oder Impfungen speichern. Auch Werte von Fitnesstrackern und anderen Wearables können dazu zählen. Die Daten werden verschlüsselt auf einem zentralen Server in Deutschland gespeichert. Per PIN-Eingabe hat der Versicherte Zugriff auf diese Daten. Eine kritische datenschutzrechtliche Prüfung erfolgt durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Bei allen Projekten fortschreitender Digitalisierung im Gesundheitswesen sind neben Medizin, Ethik und Informatik die materiellen rechtlichen Grundlagen und dabei insbesondere die datenschutzrechtlichen Aspekte zu beachten. Neben dem Behandlungserfolg steht die Hoheit des Patienten über seine Daten und deren sichere Verarbeitung stets im Vordergrund.

11.1.2 Anwendung der Datenschutz-Grundverordnung bei Arztpraxen

Aus zahlreichen Anfragen und Eingaben erfuhr der Landesbeauftragte, dass Ärzte und Zahnärzte häufig dem Irrtum unterlagen, seit der Anwendbarkeit der DS-GVO für die Datenverarbeitungen in ihren Praxen generell eine Einwilligung der Patienten zu benötigen. Einer Einwilligung bedarf es jedoch – wie auch schon vor dem 25. Mai 2018 – nicht, wenn die Datenverarbeitung erforderlich ist, um die Behandlungsverträge mit den Patienten zu erfüllen (Art. 6 Abs. 1 Satz 1 lit. b i. V. m. Art. 9 Abs. 2 lit. h DS-GVO), oder wenn eine gesetzliche Spezialnorm zu einer Datenverarbeitung befugt oder sogar verpflichtet (z. B. die Datenübermittlung zu Abrechnungszwecken zur Kassenärztlichen Vereinigung nach § 295 SGB V). Der Landesbeauftragte hat

diese Rechtsauffassung in seinem Internetauftritt veröffentlicht und auch der Ärztekammer, Zahnärztekammer und Kassenzahnärztlichen Vereinigung Sachsen-Anhalt mitgeteilt, die diese Informationen ebenfalls in ihre Publikationen aufgenommen haben.

Ärzte müssen allerdings – wie alle Verantwortlichen – ihre Informationspflichten nach Art. 13 und 14 DS-GVO erfüllen. Auch hierzu hat der Landesbeauftragte Hinweise gegeben. Die Erfüllung der Informationspflichten kann zwar durch die Unterschrift des Patienten nachgewiesen werden. Eine Unterschrift ist jedoch nicht zwingend. Insbesondere darf Patienten nicht angedroht werden, sie bei Verweigerung der Unterschrift nicht zu behandeln. Eine solche Praxis ist nicht mit der DS-GVO vereinbar. Ein Nachweis der Erfüllung der Informationspflichten (Art. 5 Abs. 2 DS-GVO) könnte auch durch das Vermerken der Aushändigung der Information oder jedenfalls das Dokumentieren eines festgelegten Verfahrensablaufs betreffend die Umsetzung der Informationspflicht erbracht werden (s. Beschluss der DSK, **Anlage 5**).

11.1.3 Anwendung der Datenschutz-Grundverordnung bei Heilpraktikern

Nach Art. 6 Abs. 1 Satz 1 lit. b i. V. m. Art. 9 Abs. 2 lit. h DS-GVO ist eine Verarbeitung von Gesundheitsdaten u. a. rechtmäßig, wenn sie aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich ist. Weitere Voraussetzung ist, dass die Daten von ärztlichem Personal oder durch sonstige Personen – die nach Unionsrecht oder dem Recht des Mitgliedstaates oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegen oder unter Verantwortung eines Gesundheitsberufsträgers agieren – verarbeitet werden (Art. 9 Abs. 3 DS-GVO i. V. m. § 22 Abs. 1 Nr. 1 lit. b BDSG).

Heilpraktiker (z. B. Osteopathen, Chiropraktiker) üben zwar einen Gesundheitsberuf aus, unterliegen jedoch weder einer unionsrechtlichen noch einer mitgliedstaatlich normierten Geheimhaltungspflicht, wie der des § 203 StGB. Zwar bestehen in diesem Berufsfeld teilweise vertraglich vereinbarte Geheimhaltungspflichten. Manche Heilpraktiker haben sich auch freiwillig einer Geheimhaltungspflicht eines Berufsverbandes unterworfen. Derartige Vereinbarungen sind nach Auffassung des Landesbeauftragten aber nicht ausreichend, da es sich hierbei nicht um eine gesetzlich geregelte Geheimhaltungspflicht handelt. Eine Datenverarbeitung ist in diesen Fällen nur auf der Grundlage einer Einwilligung möglich (Art. 9 Abs. 2 lit. a DS-GVO). Zu dieser Auffassung hat sich der Landesbeauftragte mit den weiteren Datenschutzaufsichtsbehörden in Deutschland abgestimmt. Ergebnis war eine gemeinsame Positionierung gegenüber einem Berufsverband.

11.1.4 Schulärztlicher Gesundheitsdienst

Im Rahmen der pflichtigen Schuleingangsuntersuchung wird in Sachsen-Anhalt mittels Elternfragebogen eine Vielzahl von Daten zu den einzuschulenden Kindern erhoben. Dies erfolgte trotz einer gesetzlichen Grundlage (§ 37 Abs. 2 SchulG LSA) bisher auf Einwilligungsbasis. Nunmehr soll die Datenerhebung auf der gesetzlichen Basis verpflichtend erfolgen. Der vorgesehene Umfang erscheint jedoch noch fraglich. Dies betrifft u. a. Daten zum Sozialstatus des Kindes (Schulbildung und Erwerbstätigkeit der Eltern), zum Migrationshintergrund des Kindes (Geburtsland des Kindes und der Eltern, Nationalität der Eltern), zu Geschwistern des Kindes (Anzahl Geschwister, Anzahl Geschwister im Haushalt, davon jüngere) und zum Rauchver-

halten im Haushalt (Rauchen ja/nein, Rauchen wo). Die Erforderlichkeit der Datenverarbeitung wurde aus Sicht des Öffentlichen Gesundheitsdienstes unter Bezugnahme auf Erkenntnisse vieler Studien detailliert erläutert; eine optimale Beratung benötige Daten zu den Lebensverhältnissen des Kindes, die entscheidenden Einfluss auf die Gesundheit und die psychische Entwicklung hätten. Der Landesbeauftragte überprüft die Erforderlichkeit auch unter Berücksichtigung der Verfahrensweisen und Rechtslagen in anderen Bundesländern.

11.2 Sozialwesen

Im Bereich des Sozialwesens stand im Berichtszeitraum wiederholt die Frage nach der Zulässigkeit der Erhebung und Speicherung von Kontodaten der Hilfeempfänger nach dem SGB II im Vordergrund (s. XII. Tätigkeitsbericht, Nr. 11.2.1). Die Hoffnung vieler Petenten, sich mit Hilfe des Landesbeauftragten der „Neugier“ der Jobcenter entziehen zu können, muss jedoch häufig enttäuscht werden. Die Anforderung und auch die Speicherung von Kontoauszügen sind zum Zweck der Prüfung der Leistungsvoraussetzungen auf gesetzlicher Basis in erheblichem Umfang zulässig. Dies wird durch Entscheidungen der Sozialgerichtsbarkeit bestätigt.

Entgegen der Annahme einer Petentin reicht es auch nicht aus, Kontoauszüge nur zur Einsicht vorzulegen, aber die Speicherung zu verweigern. Hierzu wies der Landesbeauftragte auf die Darlegungen des Bundessozialgerichts in der Entscheidung vom 19. September 2008 hin (Az.: B 14 AS 45/07 R, juris). Danach kann nur in einfachen Fällen von einer Speicherung abgesehen werden, im Übrigen sind die Unterlagen zu den Akten zu nehmen. Für in der Regel notwendige komplexe Einkommensberechnungen bzw. zu erwartende Nachberechnungen reicht eine kurze Einsichtnahme nach Aussage des Gerichts nicht aus.

12 Statistik

Der Zensus 2011, eine umfassende EU-weite Bevölkerungs-, Gebäude- und Wohnungszählung, war durch eine Reihe datenschutzrechtlicher Friktionen gekennzeichnet. Die seinerzeit gezogenen Lehren hatte der Landesbeauftragte in seinem XI. Tätigkeitsbericht (Nr. 12.6) dokumentiert. Die nächste Volkszählung steht bevor. Der „Zensus 2021“ ist im Kern wieder ein – grundrechtsschonendes – registergestütztes Zensusverfahren mit ergänzenden Stichprobenbefragungen in Haushalten, für die Auskunftspflicht besteht.

Im Rahmen der datenschutzrechtlichen Vorbereitung und Begleitung des Zensus 2021 war durch den Arbeitskreis Statistik der Datenschutzkonferenz eine Arbeitsgruppe gebildet worden, der der Landesbeauftragte angehört. Diese Arbeitsgruppe hatte bereits zum Entwurf eines Zensusvorbereitungsgesetzes 2021 (vgl. XIII./XIV. Tätigkeitsbericht Nr. 12.11) datenschutzrelevante Vorschläge erarbeitet und hat nun den Entwurf eines Zensusgesetzes 2021 mit dem Bundesinnenministerium erörtert. Damit sollen die Fehler der Vergangenheit, also beim Zensus 2011, beim bevorstehenden Zensus 2021 vermieden und so verhindert werden, dass in das Gesetz zur Durchführung des Zensus 2021 wieder fehlerhafte datenschutzrelevante Regelungen Eingang finden. Ein wesentlicher Kritikpunkt besteht in der weiterhin geplanten Vollerhebung bei der Gebäude- und Wohnungszählung. Darüber hinaus ist keine

anonyme Erhebung in sensiblen Sonderbereichen, wie z. B. Justizvollzugsanstalten, vorgesehen.

In das Zensusvorbereitungsgesetz 2021 wurde Ende 2018, mit Wirkung vom 13. Januar 2019, mit § 9a eine zusätzliche Regelung zur Prüfung der Übermittlungswege und der Qualität der zum Zensus 2021 zu übermittelnden Daten aus den Melderegistern sowie zum Test und zur Weiterentwicklung der Programme eingefügt. Dafür sollen die Meldebehörden den Statistischen Ämtern der Länder für alle über 82 Millionen in der Bundesrepublik gemeldeten Personen einen Datensatz von jeweils bis zu 46 teils hochsensiblen differenzierbaren Merkmalen übermitteln.

Dies ist bereits ein Verstoß gegen das Gebot der Datensparsamkeit. Die Übermittlung der Daten soll zur „Prüfung der Übermittlungswege“ erfolgen. Das heißt im Umkehrschluss, dass die verwendeten Übermittlungswege bisher ungeprüft sind. Schließlich ist auch ziemlich zweifelhaft, ob die Qualität der zum Zensus 2021 zu übermittelnden Daten aus den Melderegistern geprüft werden kann; denn der Bundesgesetzgeber hat sich bisher nicht dazu geäußert, welche Daten er beim Zensus 2021 tatsächlich erheben lassen will. Für eine solche Prüfung könnten Testdaten unter Umständen ausreichen.

Gegen den vorgesehenen Volltest mit Echtdaten wurde beim Bundesverfassungsgericht ein Antrag auf Erlass einer einstweiligen Anordnung gestellt. Mit Entscheidung vom 6. Februar 2019 (Az.: 1 BvQ 4/19, juris) wurde dieser Antrag jedoch abgelehnt. Das Bundesverfassungsgericht hat allerdings betont, dass der Ausgang eines möglichen Verfassungsbeschwerdeverfahrens damit offenbleibt.

13 Wirtschaft

13.1 Arbeitskreis Wirtschaft der Datenschutzkonferenz

Bereits im XIII./XIV. Tätigkeitsbericht (Nr. 13.1) hat der Landesbeauftragte darauf hingewiesen, dass der Düsseldorfer Kreis als Gremium der DSK unter dem Namen „Arbeitskreis Wirtschaft“ fortgeführt wird. Er befasst sich mit allgemeinen datenschutzrechtlichen Fragen aus dem Bereich der Wirtschaft, für die keine speziellen Arbeitskreise der DSK (z. B. AK Kreditwirtschaft, AK Auskunfteien, AK Versicherungswirtschaft, AK Beschäftigtendatenschutz, AK Internationaler Datenverkehr) zuständig sind.

So wurde auf Initiative des Arbeitskreises Wirtschaft der Dachverband Deutscher Immobilienverwalter e. V. durch die DSK darüber informiert, dass der Verwalter einer Wohnungseigentümergemeinschaft nicht als Auftragsverarbeiter tätig ist, sondern aufgrund eigener unternehmerischer Entscheidungen bezüglich der Verarbeitung personenbezogener Daten als Verantwortlicher. Dies bedeutet insbesondere, dass er für die Verarbeitung personenbezogener Daten einer eigenen Rechtsgrundlage bedarf und selbst die Informationspflichten erfüllen muss. Der Verband vertrat ursprünglich die Auffassung, die Tätigkeit des Verwalters sei als Auftragsverarbeitung einzustufen.

Zu weiteren datenschutzrechtlichen Themen im Zusammenhang mit der Wohnungswirtschaft siehe Nr. 13.5.

Zur Benennungspflicht von Datenschutzbeauftragten ist der Arbeitskreis Wirtschaft der Auffassung, dass für jeden Verantwortlichen nur jeweils ein Datenschutzbeauftragter zu benennen ist. Dies gilt auch für Konzerne. Wird also ein Datenschutzbeauftragter für einen Konzern benannt, ist für die konzernangehörigen Unternehmen, für die dieser Beauftragte tätig ist, kein zusätzlicher Datenschutzbeauftragter zu benennen.

13.2 Datenschutz bei kleinen und mittleren Unternehmen

Die Wirtschaft in Sachsen-Anhalt wird durch eine Vielzahl von kleinen und mittleren Unternehmen (KMU) geprägt. Für diese sind die Regelungen des Datenschutzes grundsätzlich genauso bindend wie für große Konzerne. Entscheidend für die Anwendung datenschutzrechtlicher Vorschriften ist regelmäßig weniger die Unternehmensgröße als die Art und Weise der Verarbeitung personenbezogener Daten.

Eine Ausnahme von dieser Regel besteht bei der Pflicht zur Benennung von Datenschutzbeauftragten. Abgesehen von besonderen Verarbeitungen müssen Kleinbetriebe, die nicht mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, gemäß § 38 Abs. 1 Satz 1 BDSG 2018 keinen Datenschutzbeauftragten benennen. Eine entsprechende Regelung gab es schon im alten BDSG. Auf politischer Ebene gibt es Überlegungen, die Vorschrift streichen zu lassen mit der Folge, dass viele kleine Unternehmen keinen Datenschutzbeauftragten benennen müssten. Jedoch können sich auch schon bei kleinen Unternehmen allein aus dem Umfang der Datenverarbeitung Risiken ergeben. Risiken hängen aber auch mit der Anzahl der Beschäftigten zusammen, die Daten automatisiert verarbeiten. Zudem war die bisherige Regelung weitgehend anerkannt und hat sich in der Praxis bewährt. Auch und gerade in KMU vollziehen Datenschutzbeauftragte wichtige und anspruchsvolle Tätigkeiten der Selbstkontrolle, auf die nicht verzichtet werden sollte.

Viele Anfragen und Beschwerden beim Landesbeauftragten zeigten, dass bei zahlreichen KMU Missverständnisse hinsichtlich der Auslegung der DS-GVO entstanden waren. So wurde oft behauptet, die DS-GVO verlange zur Verarbeitung personenbezogener Daten stets eine Einwilligung der betroffenen Personen. Dies ist nicht zutreffend: Die Verarbeitung personenbezogener Daten, die für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich ist, ist aufgrund von Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zulässig. Auch zur Wahrnehmung berechtigter Interessen ist eine Verarbeitung gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig, sofern nicht die Interessen der betroffenen Personen überwiegen. Sofern die Datenverarbeitung durch eine dieser Rechtsgrundlagen gerechtfertigt ist, ist das Einholen einer Einwilligung entbehrlich (zur Frage des Erfordernisses einer Einwilligung bei Arztpraxen siehe Nr. 11.1.2).

Ein weiterer Irrtum betraf die Aussage, dass jeder Angehörige eines Gesundheitsberufes zwingend einen Datenschutzbeauftragten benennen müsse. Auch das ist nicht zutreffend. In ärztlichen Einzelpraxen oder kleinen Apotheken muss regelmäßig kein Datenschutzbeauftragter benannt werden. Nähere Informationen hierzu hat die DSK in ihrem Beschluss vom April 2018 erläutert (**Anlage 1**). Natürlich steht es den Verantwortlichen frei, einen – ggf. externen – Datenschutzbeauftragten zu benennen, selbst wenn dies nicht vorgeschrieben ist.

Bereits vor Anwendung der DS-GVO ab dem 25. Mai 2018 wurde vor einer großen Abmahnwelle gewarnt. Diese Abmahnwelle ist bisher ausgeblieben. Einige wenige Gerichtsverfahren führten noch nicht zu einer einheitlichen, geschweige denn höchstrichterlichen Rechtsprechung. Noch nicht abschließend geklärt ist etwa, ob Abmahnungen von Verstößen gegen die DS-GVO durch Konkurrenten auf Grundlage des § 3a UWG oder nur auf Basis des UKlaG – z. B. durch Verbraucherschutzverbände – erfolgen können. Obwohl das Abmahnrisiko derzeit nicht groß erscheint, sollten Unternehmen darauf achten, das Risiko einer Abmahnung zu minimieren, vor allem generell die Anforderungen der DS-GVO zu erfüllen. Dies gilt u. a. für Datenschutzerklärungen auf Homepages.

13.3 Meldungen von Datenschutzverletzungen

Wie bereits im XIII./XIV. Tätigkeitsbericht (Nr. 13.4) erwähnt, sind nach Art. 33 DS-GVO alle Datenschutzverletzungen grundsätzlich der Aufsichtsbehörde zu melden. Nach der vorherigen Rechtslage war die Verletzung nur dann zu melden, wenn bestimmte sensible Datenarten betroffen waren. Daher überrascht es nicht, dass sich die Anzahl der Meldungen erhöht hat. Von Verantwortlichen allein im Wirtschaftsbereich gingen im Berichtszeitraum 2018 über 30 Meldungen beim Landesbeauftragten ein. Im gesamten Kalenderjahr 2017 waren es in diesem Bereich nur neun.

Infolge der Meldungen von Datenpannen prüft der Landesbeauftragte den Vorgang auf dessen Risikorelevanz und berät ggf. den Verantwortlichen, auch im Hinblick auf Abhilfemaßnahmen und die Benachrichtigung der betroffenen Personen.

Ein Schwerpunkt der Meldungen beinhaltete das Abhandenkommen von mobilen Datenträgern. So wurden z. B. nicht verschlüsselte Laptops aus PKW oder entlegenen Vereinsheimen entwendet. Der Landesbeauftragte wies in den betreffenden Fällen auf Folgendes hin: Werden personenbezogene Daten auf Medien gespeichert, so sind diese gemäß Art. 5 Abs. 1 lit. f DS-GVO durch geeignete technische und organisatorische Maßnahmen vor unbefugter Verarbeitung und insbesondere auch vor Verlust zu schützen. Dazu gehören eine sichere Verwahrung und die Verschlüsselung der Datenträger. Wie die datenschutzkonforme Verschlüsselung erfolgen kann, hat der Landesbeauftragte in einem Informationsblatt zusammengefasst, welches auf der Homepage abrufbar ist.[4]

Einige Meldungen erfolgten aufgrund von Fehlzustellungen von Briefpost. Sofern Briefpost nicht den angegebenen Empfänger erreicht, sollte sie umgehend dem Postdienstleister ungeöffnet zurückgegeben werden. Eine Meldung an den Landesbeauftragten erübrigt sich dann.

In einem weiteren Fall wurde die Versendung einer E-Mail durch einen Berufsgeheimnisträger an einen nichtberechtigten Empfänger gemeldet. Der Landesbeauftragte riet dringend dazu, dass Berufsgeheimnisträger (Angehörige von Heilberufen, Rechtsanwälte, Steuerberater und weitere in § 203 StGB genannte Berufsgruppen) ihren E-Mailverkehr verschlüsseln, da darin häufig sehr sensible personenbezogene Daten enthalten sind. Selbst eine versehentliche Versendung an einen Nichtberech-

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

tigten führt bei einer verschlüsselten E-Mail nicht dazu, dass personenbezogene Daten zur Kenntnis genommen werden können.

13.4 Werbung

Die DS-GVO enthält – anders als § 28 Abs. 3 und 4 sowie § 29 BDSG – keine detaillierten Regelungen zur Verarbeitung personenbezogener Daten für werbliche Zwecke. Das BDSG 2018 durfte dies nicht mehr regeln. Als Grundlage für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung zum Zwecke der Direktwerbung kommt – neben der Einwilligung (Art. 6 Abs. 1 Satz 1 lit. a DS-GVO) – in der Regel Art. 6 Abs. 1 Satz 1 lit. f DS-GVO, d. h. eine Interessenabwägung, in Betracht. Nach ErwGr 47 DS-GVO kann die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Im Rahmen der Abwägung sind jedoch die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, also deren vernünftige Erwartungen, mit zu berücksichtigen. Bei einem Werbewiderspruch wird diese Werbung unzulässig.

Durch die DSK wurde im Berichtszeitraum die Orientierungshilfe zur „Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)“ beschlossen. Sie enthält u. a. Praxisfälle zur Interessenabwägung und zur Einwilligung, beschreibt zulässige Kontaktwege zum Beworbenen und weist auf die Informationspflichten und den Werbewiderspruch hin. Sie ist auf der Homepage des Landesbeauftragten abrufbar.[5]

13.5 Wohnungswirtschaft

Im Hinblick auf die Auslegung der DS-GVO entstanden gewisse Missverständnisse und Fehlinterpretationen. So führte die öffentliche Berichterstattung zum Fall eines Wiener Wohnungsunternehmens dazu, dass Wohnungsunternehmen in Deutschland befürchteten, alle Namen ihrer Mieter von den Klingelschildern entfernen zu müssen, weil deren Einwilligungen nicht vorlagen.

Der Landesbeauftragte sah hier jedoch keinen Anlass für Rechtsunsicherheit und hat hierüber öffentlich informiert. Wie auch schon vor Anwendbarkeit der DS-GVO lässt sich die namentliche Beschilderung im Regelfall durch vertragliche Grundlagen oder berechtigte Interessen begründen. Sollten sich einzelne Mieter aus besonderen Umständen dagegen aussprechen, wäre in diesen Fällen eine andere Form der Beschilderung zu finden.

Bei Mietinteressenten und Mietern entstand mit Wirkung vom 29. November 2018 im Land Sachsen-Anhalt eine neue Befugnis für die Datenerhebung, worauf der Landesbeauftragte Wohnungsunternehmen und Verbände der Wohnungswirtschaft hingewiesen hat. Aufgrund der §§ 7, 8 Abs. 1, 9 Abs. 1 Nr. 3 Wohnraumaufsichtsgesetz hat der Vermieter nun anhand der Anzahl und des Alters der Bewohner zu prüfen, ob eine Wohnung überbelegt oder von Überbelegung bedroht ist. Bei drohender Überbelegung darf Wohnraum nicht überlassen werden, und der zugrundeliegende Vertrag wäre nach der Gesetzesbegründung gemäß § 134 BGB nichtig. Bei Bedarf kann der Vermieter jetzt von Bewohnern, die das sechste Lebensjahr noch nicht vollendet haben, das Geburtsdatum erheben.

---

[5] http://lsaurl.de/OHWerbung

Zur datenschutzrechtlichen Verantwortlichkeit des Verwalters von Wohnungseigentümergemeinschaften siehe Nr. 13.1.

14 Videoüberwachung

Die DS-GVO enthält keinen spezifischen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten mithilfe von Videotechnik. Die Rechtmäßigkeit dieser Datenverarbeitung richtet sich in der Regel nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO (vgl. ausführlich XIII./XIV. Tätigkeitsbericht Nrn. 14.1.1 und 14.1.2). Diese Vorschrift verlangt im Rahmen der Interessenabwägung ein berechtigtes Interesse der verantwortlichen Stelle. Dieses kann beispielsweise vorliegen, wenn die Videoüberwachung zum Schutz vor Einbrüchen, Diebstählen oder Vandalismus betrieben wird und dazu eine tatsächliche Gefahrenlage nachgewiesen werden kann. Die Videoüberwachung muss sich sodann auf das erforderliche Maß, z. B. bezüglich des Erfassungsbereiches und der Speicherdauer, beschränken. Zudem dürfen nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen, überwachten Personen überwiegen. Denn jede Person hat das Recht, sich in der Öffentlichkeit frei und unbeobachtet zu bewegen, ohne befürchten zu müssen, ungewollt zum Objekt einer Videoüberwachung zu werden.

Videoüberwachungen waren unverändert häufig Anlass von Beschwerden und Anfragen beim Landesbeauftragten. Dabei ging es vielfach um die Überwachung von Nachbarn, oder von öffentlichem Verkehrsraum, von Produktionsstätten und Verkaufsräumen.

In einem Einzelfall hat der Landesbeauftragte aufgrund einer Vielzahl von Beschwerden seit Herbst 2017 die Videoüberwachung eines politisch tätigen Vereins geprüft, die zunächst weiträumig den öffentlichen Raum vor einem von ihm angemieteten Gebäude erfasste. Als Begründung für die Überwachung diente die Tatsache, dass mehrfach Sachbeschädigungen erfolgten. Nach etlichen Hinweisen des Landesbeauftragten und nach Erlass einer aufsichtsbehördlichen Anordnung wurde die Videoüberwachung hinsichtlich des Erfassungsbereiches der Kameras und der Speicherdauer in erheblichem Maße eingeschränkt und im Weiteren auch die Hinweisbeschilderung an die Anforderungen der DS-GVO angepasst. Der Verein erhob gegen die Anordnung des Landesbeauftragten Klage vor dem Verwaltungsgericht. Im Dezember 2018 teilte der Verein mit, dass die aktive Videoüberwachung eingestellt und die Kameras bis zum Ende des Jahres abgebaut werden, was tatsächlich geschah.

Auf nationaler Ebene ist beabsichtigt, neben dem Kurzpapier Nr. 15 der DSK „Videoüberwachung nach der DS-GVO“, weitere Orientierungshilfen und Beschlüsse zu konkreten Anwendungsbereichen von Videoüberwachungen im Hinblick auf die DS-GVO zu überarbeiten. Der Landesbeauftragte wird diese zu gegebener Zeit auf seiner Homepage veröffentlichen.

Der Europäische Datenschutzausschuss erarbeitet eine Leitlinie zum Thema Videoüberwachung. Der Landesbeauftragte wird die Leitlinie ebenfalls veröffentlichen.

15 Verkehr

15.1 VEMAGS – Verwaltungsvereinbarung statt Staatsvertrag

Der Landesbeauftragte hatte in seinem XIII./XIV. Tätigkeitsbericht (Nr. 15.1) über die aus datenschutzrechtlicher Sicht unbefriedigende Situation nach der im Jahr 2012 erfolgten bundesweiten Einführung des ständigen Regelbetriebs für das Verfahrensmanagement für Großraum- und Schwertransporte (VEMAGS) informiert. Der vom Ministerium für Landesentwicklung und Verkehr vorgelegte damalige überarbeitete Staatsvertragsentwurf vom November 2017 beinhaltete datenschutzrechtliche Verbesserungen. Zugleich wurden innerhalb der Verkehrsressorts der Länder die rechtlichen Auswirkungen auf VEMAGS mit Hinblick auf die ab dem 25. Mai 2018 unmittelbar geltende DS-GVO diskutiert. Im Ergebnis dieses Prozesses wurde eine *vertragliche* Vereinbarung gem. Art. 26 DS-GVO zwischen den beteiligten Landesbehörden favorisiert. Diese Auslegung teilte der Landesbeauftragte nicht. Der Art. 26 DS-GVO ist eine organisatorische Regelung zur klaren Zuweisung von Verantwortlichkeiten. Er bildet keine Rechtsgrundlage bzw. kann eine Rechtsgrundlage nicht ersetzen.

Ende des Jahres 2018 informierte das Verkehrsministerium den Landesbeauftragten über den Abschluss einer „Verwaltungsvereinbarung über das Zusammenwirken zum Betrieb und zur Weiterentwicklung des Gesamtsystems Verfahrensmanagement Großraum- und Schwertransporte – VEMAGS“. Bereits im Oktober 2018 hatte die Verkehrsministerkonferenz dem Entwurf dieser Verwaltungsvereinbarung zugestimmt, mit der Maßgabe an die Gemeinsame Konferenz der Verkehrs- und Straßenbauabteilungsleiter der Länder, nach Ablauf eines Jahres eine Evaluation dieser Verwaltungsvereinbarung vorzunehmen und darüber Bericht zu erstatten.

Der Landesbeauftragte hält an seiner rechtlichen Bewertung fest. Die Evaluation der Verwaltungsvereinbarung sollte auch die Frage nach der datenschutzrechtlichen Grundlage beantworten.

15.2 Kontrolle der Dieselfahrverbote

Der sogenannte „Diesel- oder Abgasskandal“, d. h. eine Reihe bewusster Manipulationen an der Motorsteuerung durch verschiedene Autohersteller zur Umgehung gesetzlich vorgegebener Grenzwerte für Autoabgase bei Dieselkraftfahrzeugen durch softwaregesteuerte Abschalteinrichtungen, hat auch ein datenschutzrechtliches Nachspiel. Der Vorgang zeigt exemplarisch, wie wichtig die Beachtung datenschutzrechtlicher Grundsätze ist.

Gegen den Entwurf der Bundesregierung eines Neunten Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 15. November 2018 (BR-Drs. 574/18), hier insbesondere des neuen § 63c StVG, bestehen verfassungsrechtliche Bedenken. Obwohl der Gesetzentwurf in seiner Begründung auf das Urteil des Bundesverfassungsgerichts zum Kennzeichenscanning (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05 und 1 BvR 1254/07) verweist, werden dessen Vorgaben nicht eingehalten. Das vorgesehene Fahrverbot für Dieselfahrzeuge soll durch eine weiträumige automatisierte Erfassung mittels Kennzeichenlesegeräten überwacht werden. Dabei erfolgt nicht nur der Abgleich des Halters und der Fahrzeugdaten, sondern auch die Erhebung eines Bildes des Fahrers. Die Regelung erfasst unterschieds- und anlasslos alle Fahrzeug-

führer und Kraftfahrzeuge, die sich – rechtmäßig oder rechtswidrig – innerhalb von Verbotszonen bewegen, die gemäß § 40 des Bundes-Immissionsschutzgesetzes zum Schutze der Bevölkerung vor Abgasen durch die Straßenverkehrsbehörden im Einvernehmen mit den für den Immissionsschutz zuständigen Behörden eingerichtet wurden bzw. eingerichtet werden können.

Diese automatische Erfassung aller Halter- und Fahrzeugdaten ohne unverzügliche Auswertung und Löschung auch im sog. „Nichttrefferfall“ (worauf es aber nach der jüngsten Rechtsprechung des Bundesverfassungsgerichts gar nicht mehr ankommt, denn das Gericht hat seine o. a. Entscheidung weiterentwickelt und auch im „Nichttrefferfall“ einen Eingriff bejaht, siehe Beschlüsse vom 18. Dezember 2018, 1 BvR 2795/09, 1 BvR 3187/10 und 1 BvR 142/15) greift in das Grundrecht auf informationelle Selbstbestimmung ein.

Die nicht näher begründete vorgesehene Speicherfrist von sechs Monaten für die Daten der vom Fahrverbot betroffenen Dieselfahrzeuge geht erheblich über die bestehende Verjährungsfrist von drei Monaten für Verkehrsordnungswidrigkeiten hinaus.

Dieses Gesetzesvorhaben ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Mit diesem Ansatz ist man von einer umfassenden automatisierten Überwachung des Straßenverkehrs nur noch wenige Schritte entfernt. Mit der Einführung einer „blauen“ Plakette, die signalisieren würde, dass das Kraftfahrzeug den erforderlichen Umweltstandards genügt, könnte dieser Eingriff in das informationelle Selbstbestimmungsrecht von Millionen Verkehrsteilnehmern vermieden werden. Damit wäre die geplante gesetzliche Regelung nicht erforderlich und letztlich überflüssig.

Die Neuregelung soll auch verdeckte Datenerhebungen ermöglichen. Zwar nur unter der Einschränkung, dass dies nur zulässig sein soll, wenn durch die offene Datenerhebung der Zweck der Maßnahme konkret und erheblich gefährdet wäre. Aber allein gegen die Einräumung der Möglichkeit einer verdeckten Datenerhebung bestehen ebenfalls verfassungsrechtliche Bedenken. Eine verdeckte Datenerhebung bedeutet, dass für den Betroffenen nicht erkennbar wird, dass überhaupt Daten von ihm erhoben werden. Hierdurch ist es den betroffenen Verkehrsteilnehmern auch nicht möglich, hiergegen gerichtlich vorzugehen. Um der Rechtsweggarantie des Art. 19 Abs. 4 GG Genüge zu tun, müsste zumindest eine nachträgliche Information über die verdeckte Datenerhebung erfolgen. Eine solche ist aber in dem Gesetzentwurf nicht vorgesehen.

Eine verdeckte Datenerhebung intensiviert zudem den Grundrechtseingriff und kann zur Verfolgung einer Verkehrsordnungswidrigkeit (bei einem Bußgeldrahmen von 25 bis 80 €) nicht gerechtfertigt sein. Selbst Mautüberwachungsstationen sind als solche im Verkehrsraum erkennbar. Hier können bei Verstößen gegen die Zahlung einer Mautgebühr sogar Bußgelder von bis zu 20.000 € erhoben werden.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wurde vom Bundesministerium für Verkehr und digitale Infrastruktur an der Ressortabstimmung beteiligt. Dadurch konnte zumindest erreicht werden, dass im Gesetzentwurf die *offene* Datenerhebung durch die Verkehrskontrollbehörde der Regelfall ist. Die seitens der Bundesregierung anfänglich vorgesehene Speicherdauer von zwei Jahren konn-

te zudem durch die Intervention der Bundesbeauftragten zumindest auf sechs Monate im Gesetzentwurf begrenzt werden.

Die Landesbeauftragten für den Datenschutz wurden im Prozess der Vorabstimmung und auch im Bundesratsverfahren durch die zuständigen Landesverkehrsministerien nicht einbezogen. Der Bundesrat nahm einige der o. a. Kritikpunkte in seiner Stellungnahme vom 14. Dezember 2018 auf und lehnte den Gesetzentwurf ab (BR-Drs. 574/18 (Beschluss)).

Berichten zufolge will die Bundespolitik ihre Pläne zur automatisierten Kontrolle von Dieselfahrverboten aus Datenschutzgründen doch noch etwas zurücknehmen. Bei den Kontrollen soll es sich lediglich um Stichproben mit mobilen Geräten handeln. Die Daten sollen zudem bereits zwei Wochen nach der Erhebung gelöscht werden. Es werde keine Massenüberwachung geben.

Es bleibt mit gewisser Skepsis abzuwarten, mit welcher Lösung der Bundesgesetzgeber eine datenschutzgerechte Überprüfung der Dieselfahrverbote vornimmt.

Anlagen

Anlage 1

Beschluss der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25. und 26. April 2018 in Düsseldorf

Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. c Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z. B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

Anlage 2

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 3

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf

Beschluss der DSK zu Facebook Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst.“

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Art. 26 Abs. 1 DSGVO)

2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DSGVO nachkommt?

3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?

4. Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DSGVO, auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DSGVO und auf Auskunft nach Art. 15 DSGVO?

5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?

6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?

7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?

8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

Anlage 4

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf

Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien

Die Konferenz nimmt das Ergebnis der Beratungen des Arbeitskreises Grundsatzfragen des Datenschutzes zur Kenntnis und empfiehlt für die weitere Rechtspraxis, die im Folgenden aufgeführten Positionierungen bei der Tätigkeit als Aufsichtsbehörde zu Grunde zu legen:

1. Soweit Datenverarbeitungen von Parlamenten (auch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die DSGVO keine Anwendung.

2. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.

3. Die Einordnung von Tätigkeiten der Parlamente (auch deren Organe einschließlich der Abgeordneten) als verwaltende und fiskalische in Abgrenzung zur parlamentarischen Kerntätigkeit bedarf jeweils einer Bewertung im Einzelfall.

4. Soweit keine gesetzlichen Grundlagen für die parlamentarische Kerntätigkeit bestehen, wäre eine Datenschutzordnung des Parlaments zu empfehlen, die sich an der DSGVO orientieren sollte. Eine Beratung durch die Aufsichtsbehörde sollte in jedem Fall unbenommen bleiben.

5. Parteien als nicht-öffentliche Stellen sind grundsätzlich Normadressaten der DSGVO und unterliegen damit der Aufsicht der Aufsichtsbehörden. Eine mögliche Berücksichtigung ihres besonderen Status im Rahmen der Gesetzesanwendung bleibt unberührt.

Anlage 5

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf

Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DSGVO durch Unterschrift zu bestätigen

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sprechen sich dagegen aus, dass Ärztinnen und Ärzte oder andere Angehörige von Gesundheitsberufen die Behandlung ablehnen oder die Verweigerung der Behandlung androhen, wenn die Patientin oder der Patient die Informationen nach Art. 13 DSGVO nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist nicht mit der DSGVO vereinbar.

Die Informationspflicht nach Art. 13 DSGVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte.

Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.

Anlage 6

Entschließung der 96. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 7. und 8. November 2018 in Münster

Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die DSK weist hierzu auf die kritische Stellungnahme[6] des Europäischen Datenschutzausschusses hin. Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch kei-

---

[6] https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de

ne Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden. Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z.B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u.a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

Anlage 7

Organigramm

Stichwortverzeichnis

S

T

V

W

Z