SACHSEN-ANHALT

XVII. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz

Telefon: 0391 81803-0
Fax: 0391 81803-33

Internet: https://datenschutz.sachsen-anhalt.de/
E-Mail: poststelle@lfd.sachsen-anhalt.de

Anschrift: Postfach 1947, 39009 Magdeburg
Dienstgebäude: Otto-von-Guericke-Str. 34a, 39104 Magdeburg

Vorwort

Dieser XVII. Tätigkeitsbericht umfasst den Zeitraum vom 1. Januar 2020 bis zum 31. Dezember 2020. Inhaltlich fällt er in die Amtszeit meines Vorgängers Dr. Harald von Bose, der am 31. Dezember 2020 in den Ruhestand gegangen ist. Dr. Harald von Bose hat sich für den Datenschutz im Land Sachsen-Anhalt in hohem Maße eingesetzt. Seinem großen Engagement im Datenschutz ist es zu verdanken, dass das Land Sachsen-Anhalt im Datenschutz auch bundesweit eine Rolle gespielt hat. Er hat sich außerdem für die Weiterentwicklung des Datenschutzes in Sachsen-Anhalt außerordentlich verdient gemacht. Die Dienststelle ist ihm deshalb im besonderen Maße zu Dank verpflichtet.

Die Vertretung im Amt übernahm für die Zeit vom 1. Januar 2021 bis 31. Juli 2024 der Direktor der Dienststelle, Albert Cohaus. Herr Cohaus hat sich außerordentlich für die Geschäftsstelle eingesetzt. Am 1. August 2024 habe ich dann die Amtsgeschäfte übernommen. Ich war am 24. April 2024 vom Landtag Sachsen-Anhalt von den anwesenden Abgeordneten mit 66 Ja-Stimmen, 26 Gegenstimmen und zwei Enthaltungen, gewählt worden. Mit dieser Wahl fand die Vakanz im Amte des beziehungsweise der Landesbeauftragten ein Ende.

Zu einer meinen Aufgaben gehört es nun unter anderem, die Tätigkeitsberichte der Jahre 2020 bis 2023 zu erstellen, um einen Überblick über die Tätigkeit der Jahre 2020 bis 2023 zu gewährleisten. Der Tätigkeitsbericht für das Jahr 2020 wurde mir schon nahezu fertig vorgelegt, so dass dieser nun separat veröffentlicht wird. Die Jahre 2021 bis 2023 werden gemeinsam veröffentlicht und der Tätigkeitsbericht über das Jahr 2024 wird dann mein erster Tätigkeitsbericht sein, der einen Teilzeitraum in meinem Amt umfasst.

Ich habe den Tätigkeitsbericht für das Jahr 2020 in der Formulierung in der Form des Landesbeauftragten belassen. Dieser XVII. Tätigkeitsbericht bietet einen Überblick über das Jahr 2020. Es können Themen darunter sein, die im Jahr 2025 nicht mehr aktuell zu sein scheinen. Doch auch die sind wichtig, um im Falle einer wiederkehrenden Situation Anhaltspunkte für die Lösung zu erhalten.

Der Brexit und seine Folgeprobleme sind einer der Punkte, der eher keine Wiederholung finden wird.

Während wir heute mit Sorge auf das EU-Privacy Framework schauen, mussten wir uns 2020 nach Safe Harbor mit den Folgen des EuGH-Urteils „Schrems II“ für das E-Privacy-Shield und den Anforderungen an die Datenübermittlung in Drittländer befassen (Kapitel 5.2-5.3).

Schon im Jahr 2020 hat sich der Landesbeauftragte mit dem Thema Microsoft Office 365 und den datenschutzrechtlichen Heraus- und Anforderungen befasst (Kapitel 6.8).

Datenschutz an Schulen ist ein weiterer Kernbereich dieses Tätigkeitsberichts, dessen Bestandteile nach wie vor von großem Interesse sind (Kapitel 12). Dazu kommen Informationen und Fallbespiele zum Thema Datenpannen (Kapitel 14.2.2, 16.1). Die DSK hat 2020 eine Orientierungshilfe zur „Videoüberwachung durch nicht-öffentliche

Stellen“ herausgegeben. Hiermit befasst sich der Tätigkeitsbericht sowie mit Fallbeispielen aus dem Bereich der Videoüberwachung im nicht-öffentlichen Bereich (Kapitel 17).

Kapitel 4.4 befasst sich mit der Zentralisierung der Datenschutzaufsicht für den Markt und setzt sich mit dem Streitstand auseinander.

Einen Rückblick auf die besondere Situation der Corona-Pandemie und deren datenschutzrechtliche Herausforderungen darf im XVII. Tätigkeitsbericht natürlich nicht fehlen (Kapitel 13).

Ich wünsche eine erkenntnisreiche Lektüre. Zur besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnung gelten gleichermaßen für alle Geschlechter.

Magdeburg, den 31. April 2025

Maria Christina Rost
Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

Anlagenverzeichnis

Abkürzungsverzeichnis

A

Abs.	Absatz
AG InfoSic	Arbeitsgruppe Informationssicherheit
AK	Arbeitskreis
AktO	Aktenordnung
AMG	Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz)
AO	Abgabenordnung
AöR	Anstalt öffentlichen Rechts
ApBetrO	Verordnung über den Betrieb von Apotheken (Apothekenbetriebsordnung)
Art.	Artikel
a. F.	alte Fassung

B

BAföG	Bundesausbildungsförderungsgesetz
BCM	Business Continuity Management, Betriebliches Kontinuitätsmanagement
BCR	Binding Corporate Rules, verbindliche interne Datenschutzvorschriften
BDSG	Bundesdatenschutzgesetz
beA	besonderes elektronisches Anwaltspostfach
beBPo	besonderes elektronisches Behördenpostfach
beN	besonderes elektronisches Notarpostfach
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BLSA	Landesbetrieb Bau- und Liegenschaftsmanagement Sachsen-Anhalt
BMI	Bundesministerium des Innern, für Bau und Heimat
BORA	Berufsordnung für Rechtsanwälte
BR	Bundesrat
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestagsdrucksache

C

CIO	Chief Information Officer, Leiter Informationstechnik
CISO	Chief Information Security Officer, Gesamtverantwortlicher für die Informationssicherheit in einer Organisation
CON.2	Datenschutz-Baustein aus dem IT-Grundschutz-Kompendium

D

DAkkS	Deutsche Akkreditierungsstelle GmbH
DANE	DNS-based Authentication of Named Entities, Netzwerkprotokoll zur sicheren Datenübertragung im Internet
De-Mail	Auf E-Mail-Technik beruhendes Kommunikationsmittel zur sicheren, vertraulichen und nachweisbaren Kommunikation im Internet
DEK	Datenethikkommission
DIN	Deutsches Institut für Normung e. V.
DNS	Domain Name System, weltweiter Verzeichnisdienst, der den Namensraum des Internets verwaltet
DNSSEC	DNS-based Authentication of Named Entities bindet einen E-Mail-Server an ein im DNS installiertes (Fingerprint) Zertifikat, wobei mittels DNSSEC-signiertem DNS-Eintrag die Unterstützung von STARTTLS angezeigt und ein Downgrade auf unverschlüsselte Übertragung verboten wird.
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt)
DPA	Data Processing Addendum, Datenschutzbestimmungen
DSB	Datenschutzbeauftragter
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
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

eBO	elektronisches Bürger- und Organisationen-Postfach
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EDPB	European Data Protection Board, Europäischer Datenschutzausschuss, s. EDSA
EDPS	European Data Protection Supervisor, s. EDSB
EGovG LSA	Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt)
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
EN	Europäische Norm
ERV	Elektronischer Rechtsverkehr
ERVV	Elektronischer-Rechtsverkehr-Verordnung

ERVVO LSA	Verordnung über den elektronischen Rechtsverkehr bei den Gerichten und Staatsanwaltschaften des Landes Sachsen-Anhalt
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-KOM	Europäische Kommission
e. V.	eingetragener Verein

F

ff.	fortfolgende
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnis-Verordnung – FeV)
FITKO	Föderale IT-Kooperation

G

GAIA-X	Projekt zum Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa
GDG LSA	Gesetz über den Öffentlichen Gesundheitsdienst und die Berufsausübung im Gesundheitswesen im Land Sachsen-Anhalt (Gesundheitsdienstgesetz)
GDPR	General Data Protection Regulation (dt.: Datenschutz-Grundverordnung, s. DS-GVO)
GenG	Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften (Genossenschaftsgesetz)
GG	Grundgesetz
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum für polizeiliche Telekommunikationsüberwachung
GO LSA	Gemeindeordnung für das Land Sachsen-Anhalt
GPA	Global Privacy Assembly, Internationale Datenschutzkonferenz
GWB	Gesetz gegen Wettbewerbsbeschränkungen

H

HGB	Handelsgesetzbuch
HPI	Hasso-Plattner-Institut
HwO	Handwerksordnung

I

ICO	Information Commissioner’s Office, Datenschutzaufsichtsbehörde des Vereinigten Königreichs
IETF	Internet Engineering Task Force, Internettechnik-Arbeitsgruppe, eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst
IfSG	Infektionsschutzgesetz
IKT	Informations- und Kommunikationstechnik
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
ISM	Informationssicherheitsmanagement

ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ISRL	Informationssicherheitsrichtlinie
IT	Informationstechnik
ITN	Informationstechnisches Netz (des Landes Sachsen-Anhalt)
ITN-XT	ITN der nächsten Generation (XT: next generation)

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
JITG LSA	Justiz-IT-Gesetz

K

KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
KVG LSA	Kommunalverfassungsgesetz des Landes Sachsen-Anhalt

L

LISL LSA	Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt, Informationssicherheitsleitlinie
lit.	lat. littera (Buchstabe)
LT-Drs.	Landtagsdrucksache
LUGAS	Länderübergreifendes Glücksspielauswertesystem

M

MDR	Mitteldeutscher Rundfunk
MPU	Medizinisch-Psychologische Untersuchung
MStV	Medienstaatsvertrag
MTA	Mail Transfer/Transport Agent ist ein Programm auf dem E-Mail-Server zur Verteilung von E-Mail
MTA-STS	Mail Transfer Agent – Strict Transport Security, Standard der IETF nutzt Zertifikate auf E-Mail- und Webserver mit DNSSEC-signiertem DNS-Eintrag

N

Nr.	Nummer
NOYB	None Of Your Business („geht dich nichts an“), europäisches Zentrum für digitale Rechte, Nichtregierungsorganisation

O

OECD	Organisation for Economic Co-operation and Development, Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OSCI	Online Services Computer Interface (OSCI), Sammlung von Netzwerkprotokollen für die deutsche öffentliche Verwaltung
OSCI-Transport	Protokollstandard zur vertraulichen und sicheren Übermittlung von Nachrichten
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz)

P

PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz)
PDCA-Zyklus	„Plan - Do - Check - Act“-Zyklus nach W. E. Deming
PDSG	Patientendaten-Schutz-Gesetz
PStG	Personenstandsgesetz

R

RegMoG	Registermodernisierungsgesetz
RettDG LSA	Rettungsdienstgesetz des Landes Sachsen-Anhalt
Rn.	Randnummer

S

SaaS	Software as a Service, in der Cloud betriebene Software
SAFE	Name einer Software zum Betrieb eines Verzeichnisdienstes und Standard für Verzeichnisdienste (Adressbücher), das beBPo kann den SAFE-Verzeichnisdienst der Justiz nutzen
SARS-CoV-2	severe acute respiratory syndrome coronavirus type 2, schweres akutes Atemwegssyndrom Coronavirus Typ 2, umgangssprachlich (neuartiges) Coronavirus
SARS-CoV-2-EindV	Verordnung über die Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt
„Schrems II“-Urteil	Urteil des EuGH, Az. C-311/18
SCC	Standard Contractual Clauses, Standarddatenschutzklauseln
SchfHwG	Schornsteinfeger-Handwerksgesetz
SchulDatSchVO	Verordnung über den Schutz personenbezogener Daten im Schulwesen des Landes Sachsen-Anhalt
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SDM	Standard-Datenschutzmodell
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung

SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz
S/MIME	Secure / Multipurpose Internet Mail Extensions, Standard für Verschlüsselung und Signieren von MIME-Objekten durch ein hybrides Kryptosystem
SMTP	Simple Mail Transfer Protocol, Einfaches E-Mail-Transport-Protokoll
sog.	sogenannte
SSL	Secure Sockets Layer, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (ehem. Bez., s. TLS)
STARTTLS	Schlüsselwort, das den Wunsch nach Nutzung einer TLS-basierten Verschlüsselung signalisiert
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz

T

TCA	Trade and Cooperation Agreement, Handels- und Kooperationsabkommen (zwischen der Europäischen Union und dem Vereinigten Königreich)
TIA	Transfer Impact Assessments, Risikoanalysen und Folgenabschätzungen, bezogen auf den jeweiligen Datentransfer
TLS	Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
TMG	Telemediengesetz

U

UAG	Unterarbeitsgruppe
UAK	Unterarbeitskreis
UAS	Unmanned Aircraft System
UK	United Kingdom, Vereinigtes Königreich
US/USA	United States of America, Vereinigte Staaten von Amerika
u. a.	unter anderem

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
vgl.	vergleiche
VPN	Virtual Private Network
VwV	Verwaltungsvorschrift
VZBV	Verbraucherzentrale Bundesverband e. V.

W

WAN	Wide Area Network

Z

ZPO	Zivilprozessordnung

1 Einführung

1.1 Künstliche Intelligenz

Während innovative KI-Technologien die wirtschaftliche Entwicklung fördern, bietet diese sowohl Chancen als auch Risiken. Die Nationale KI-Strategie der Bundesregierung gibt die wesentlichen Rahmenbedingungen vor, um „Artificial Intelligence (AI) made in Germany“ zu einem weltweit anerkannten Gütesiegel werden zu lassen. Um KI immer im Dienste und zum Wohle der Menschen einzusetzen, sind insbesondere die Achtung der Menschenwürde und der Schutz personenbezogener Daten bei der Nutzung notwendig. Nur so kann KI zu einem Standort- und Wettbewerbsvorteil werden.

Der Deutsche Bundestag hat sich mit Bildung der Enquete-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ des Themas KI angenommen. Die Kommission setzte sich zu gleichen Teilen aus Mitgliedern des Deutschen Bundestags und externen Experten zusammen. Ihre Aufgabe war die Untersuchung des KI-Einflusses auf Gesellschaft, Wirtschaft und Arbeitswelt und den Staat. Eine große Anzahl technischer, rechtlicher und ethischer Fragen wurde aufgegriffen und auch der staatliche Handlungsbedarf identifiziert und beschrieben. Chancen sollen erkannt und genutzt werden können, Risiken sollen minimiert werden. Am 28. Oktober 2020 übergab die Enquete-Kommission ihren 800-seitigen Abschlussbericht (BT-Drs. 19/23700)[1] an den Bundestagspräsidenten. Die Kommission thematisierte „KI und Wirtschaft“, „KI und Staat“, „KI und Gesundheit“, „KI und Arbeit, Bildung, Forschung“, „KI und Mobilität“ sowie „KI und Medien“.

Die Landesregierung definierte mit der Digitalen Agenda[2] des Landes Sachsen-Anhalt eigene strategische Ziele und konkrete Maßnahmen für die Digitalisierung des Landes. Sie setzt sich in diesem Rahmen für die Nutzung von moderner und datenschutzgerechter KI im Land ein. Die Digitale Agenda stammt noch aus dem Dezember 2017. Federführend verantwortlich ist das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt. Die 130 enthaltenen Maßnahmen sollen gemeinsam von allen Ministerien und ihren Geschäftsbereichen, also der gesamten Landesverwaltung, umgesetzt werden. Der Großteil befindet sich noch in der Umsetzung, jedoch gibt es auch bereits erfolgreich abgeschlossene Maßnahmen. Die Stakeholder haben den stetigen Wandel im Blick und für 2021 eine Fortschreibung im Sinne einer Nachjustierung und Ergänzung angekündigt.

Im Tätigkeitsbericht des vorigen Berichtszeitraums wurde der Fokus auf das Thema KI als Teil der Digitalen Agenda des Landes in der Erwartung gelegt, dass diese zukünftig eine herausragende und prägende Rolle spielen wird. Die Empfehlungen des Landesbeauftragten aus dem XVI. Tätigkeitsbericht (Nr. 1.2) haben weiterhin Bestand.

Jede Nutzung von KI benötigt große Datenmengen zu Lernzwecken, z. B. um Software zu trainieren und Regeln für Entscheidungen abzuleiten. Die Sammlung von unveränderten Rohdaten ohne Zweck und Rechtsgrundlage auf Vorrat ist in der öffentlichen Verwaltung und im nichtöffentlichen Bereich gleichermaßen datenschutzrechtlich nicht

---

[1] https://dip21.bundestag.de/dip21/btd/19/237/1923700.pdf

[2] https://digital.sachsen-anhalt.de/

zulässig. Hier müssen Daten sparsam, minimal und zielorientiert auf Basis einer Rechtsgrundlage erhoben, verarbeitet und anschließend zeitnah auch wieder gelöscht werden.

Künstliche Intelligenz ist gleichwohl eine Zukunftstechnologie, deren Chancen aktiv genutzt werden sollten. Die Beschaffung und Nutzung von unter dem Aspekt der Datensparsamkeit erhobenen Daten ist jedoch nicht ohne Weiteres mit KI-Erfordernissen vereinbar. Der Bitkom e. V. schlägt daher vor, um nicht dauerhaft auf die Nutzung kostbarer Daten verzichten zu müssen, den Fokus des Datenschutzes stärker auf Datenverfügbarkeit und Datensouveränität als auf Datensparsamkeit zu legen. Der Landesbeauftragte sieht hierin eine Herausforderung für die Politikerinnen und Politiker in Bund und Land, auch in Europa, eine datenschutzgerechte KI legislativ zu ermöglichen.

Datenschutzgerechte KI ist möglich, muss jedoch von Anfang an in der Produktentwicklung eingeplant und feinfühlig umgesetzt werden. So sind oftmals problemlos auch anonymisierte Daten, z. B. bei Kameradaten von autonomen Fahrzeugen, nutzbar. Gleichzeitig ist der Grad der Anonymisierung genau passend einzustellen, da das ggf. Auswirkungen auf das Ergebnis der KI haben kann. So kann eine KI-basierte Untersuchung von Bildern und Proben in der Medizin beispielsweise zur Krebsdiagnose durchaus auf exakte Geburtsdaten verzichten, ein Verzicht auf das Geburtsjahr selbst könnte bereits zu Ungenauigkeiten im Ergebnis führen.

Die technische Entwicklung hat die durch das bestehende Datenschutzrecht gegebenen Möglichkeiten schon lange überholt. Produkte aller Art verwenden KI und werden frei verkauft. Der Nutzer ist für die datenschutzgerechte Installation verantwortlich, jedoch ist dies dem Anwender oft gar nicht bewusst. Oft ist unbekannt, was die Produkte können, auf welche Datenquellen per Internet zugegriffen wird, welche Daten in der Cloud verarbeitet werden, was im Gerät geschieht oder dass etwa KI überhaupt genutzt wird. Wie und wovon hat diese gelernt? Wurden diskriminierende Schwerpunkte gelernt? Werden Personengruppen oder Einzelaspekte bevorzugt oder benachteiligt?

Auch in der öffentlichen Verwaltung werden große Erwartungen an den Einsatz von KI geknüpft. Es fehlen jedoch noch immer hinreichend konkrete Anwendungsszenarien und damit verbundene Konzepte zu Umfang und Inhalt sowie zur Verwaltung und Pflege von Datenquellen für Big Data-Anwendungen. Zielstellung ist unter anderem die Vermeidung der Weitergabe von Daten an Dienstleister außerhalb des Geltungsbereichs der DS-GVO.

Der Landesbeauftragte macht sich für den Aufbau eines ressortübergreifenden Kompetenzteams KI im Land stark, das bestehendes Wissen konzentriert, Nutzungsszenarien testet und beratend möglichen Nutzern zur Seite steht.

1.2 Digitale Souveränität

Idealerweise sollte das Hauptkriterium für den Einsatz bestimmter Soft- und Hardware deren Zweckmäßigkeit zur Bewältigung einer bestimmten Aufgabe oder Zielstellung im konkreten Anwendungsfall sein. Dazu zählt unter Umständen auch die Kompatibilität zu Lösungen, die von Partnern und Kunden, Behörden und Bürgern, Familie und Freunden verwendet werden. Aus datenschutzrechtlicher Sicht gehört zu dieser

Zweckmäßigkeit selbstverständlich auch die prinzipielle Möglichkeit der Gestaltung eines DS-GVO-konformen Einsatzes der in Frage stehenden Lösung und deren konsequente Umsetzung.

Nicht erst seit dem pandemiebedingt sprunghaften Anstieg der Nutzung von Telearbeitsplätzen (Home-Office, Wohnraumarbeit) und digitalen Kommunikationsmitteln im Allgemeinen, sind Defizite bzgl. dieser Gestaltungsfreiheit bekannt. Diese unerwartet rasche Entwicklung führte jedoch dazu, dass die Defizite deutlicher und umfassender zu Tage treten konnten. Die seit längerem häufig beklagte Monopolstellung einiger weniger Technologiekonzerne auf dem Gebiet der Computerbetriebssysteme und allgemeiner Büro-, Geschäfts- und Kommunikationssoftware bedingt nicht nur wirtschaftliche Konsequenzen. Im Zusammenhang mit der zunehmenden Abhängigkeit aller Bereiche des gesellschaftlichen Lebens von vernetzter Kommunikation offenbart die Marktbeherrschung einiger weniger Akteure auch eine gewaltige datenschutzrechtliche Dimension, vor allem aufgrund der Tatsache, dass das unternehmerische Zentrum dieser Akteure häufig außerhalb des Geltungsbereiches der DS-GVO liegt.

Bereits im XVI. Tätigkeitsbericht (Nr. 1.3) wurde darauf hingewiesen, dass digitale Souveränität nicht nur die konkrete Soft- und Hardware betrifft, sondern auch Datenformate und Schnittstellen nach allgemeinen Standards bzw. den Zugriff auf Quellcodes und die freie Auswahl von Dienstleistern einschließt. Als allgemein bekanntes Beispiel für Quasi-Monopolstellungen wurde dort die Firma Microsoft genannt. An dieser Situation hat sich in der Praxis leider nichts geändert. Allerdings sollten weiterhin Hoffnungen in Projekte wie GAIA-X oder die Bestrebungen nach vermehrtem Einsatz von Open-Source-Software auch in der öffentlichen Verwaltung gesetzt werden, auch wenn deren aktuelle Auswirkungen noch kaum spürbar sind.

Der IT-Planungsrat hat in einer „Strategie zur Stärkung der Digitalen Souveränität für die IT der öffentlichen Verwaltung“ Ziel- und Handlungsfelder aufgezeigt, die die öffentliche Verwaltung als Nutzer, Bereitsteller und Auftraggeber digitaler Technologie in den Blickpunkt rücken.[3]

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben der datenschutzrechtlichen Bedeutung der Digitalen Souveränität mit der am 22. September 2020 verabschiedeten Entschließung „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen“ Nachdruck verliehen **(Anlage 5)**.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die Tätigkeit des Landesbeauftragten war im Berichtszeitraum von der Corona-Pandemie geprägt. Beratungen von Verantwortlichen, die unter normalen Umständen im persönlichen Gespräch stattgefunden hätten, mussten telefonisch oder auf schriftlichen Wege durchgeführt werden. Vor-Ort-Kontrollen konnten nicht im gewünschten

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

Maß durchgeführt werden. In den Fällen, in denen sie nicht kompensiert werden konnten, werden sie nachgeholt, sobald es die Pandemielage zulässt. Beratungen der Datenschutzkonferenz und deren Arbeitsgruppen wurden ab März 2020 online mithilfe von Videokonferenzsystemen durchgeführt. Gleiches galt für Vorträge und die Teilnahme an Beratungen von betrieblichen Datenschutzbeauftragten. Die turnusmäßige Beratung des Landesbeauftragten mit den Kammern fand ebenfalls in einem Onlineformat statt. Dabei konnte festgestellt werden, dass auch datenschutzfreundliche Konferenzsysteme zuverlässig und komfortabel zu nutzen sind. Trotz der Einschränkungen ist es gelungen, für das Aus- und Fortbildungsinstitut des Landes einzelne Präsenzveranstaltungen durchzuführen, insbesondere im Rahmen des Beschäftigtenlehrgangs II.

Viele Verantwortliche haben sich offenbar mittlerweile vertieft mit der seit Mai 2018 geltenden neuen Rechtslage befasst. Dies zeigen zahlreiche Anfragen, die sehr differenziert spezielle datenschutzrechtliche Probleme aufwarfen. Gerade bei der Bearbeitung von Beschwerden wurden aber auch gravierende Mängel bekannt, die auf fehlende Grundkenntnisse oder fehlenden Umsetzungswillen im Bereich des Datenschutzes hindeuteten. Mitunter waren Verantwortliche sehr zögerlich mit der Beantwortung von Auskunftsersuchen, worauf der Landesbeauftragte Auskunftsbescheide erließ. In einem Fall wurde ein Auskunftsbescheid mit einer Klage angefochten, in dem einem Verantwortlichen 15 Fragen zur Videoüberwachung gestellt wurden. Das Verwaltungsgericht Magdeburg stellte fest, dass alle 15 Fragen aufgrund der Untersuchungsbefugnis des Landesbeauftragten gemäß Art. 58 Abs. 1 lit. a DS-GVO gestellt werden durften. Nach dieser Vorschrift kann der Landesbeauftragte Verantwortliche anweisen, ihm alle Informationen bereitzustellen, die für die Erfüllung seiner Aufgaben erforderlich sind.

Im Berichtszeitraum wurde das Online-Angebot des Landesbeauftragten deutlich erweitert und aktualisiert. So stellte er auf seiner Homepage zahlreiche neue Informationen bereit, insbesondere für Verantwortliche des Gesundheitsbereichs sowie für die Bereiche der Werbung und der Videoüberwachung. Zudem erfolgten Informationen zu vom EDSA verabschiedeten Leitlinien, Handreichungen zum Export von Daten in Staaten außerhalb der EU sowie Informationen und Empfehlungen zur Bewältigung des Brexits. Aktualisiert wurde das Informationsblatt „Häufig gestellte Fragen zum Datenschutz in Vereinen“. Im Zusammenhang mit der Corona-Pandemie sind viele unterschiedliche Fragestellungen entstanden, zu denen auf der Homepage Hinweise und Hilfen gegeben werden konnten (siehe Kap. 13).

Erneut zugenommen hat die Anzahl der Beschwerden. Inhaltliche Schwerpunkte waren die fehlerhafte Erfüllung der Betroffenenrechte (wie im Vorjahr) und die Videoüberwachung. Hier kam es zu einer Zunahme schriftlicher Verfahren von deutlich über 25%.

Auch die Anzahl der Meldungen von Datenschutzverletzungen ist weiterhin hoch. Das Spektrum dieser Verletzungen reicht von einfachen Fehlversendungen, die in sensiblen Bereichen (Gesundheitsdaten, Sozialdaten) durchaus gravierende Auswirkungen haben können, bis hin zu komplexen Schädigungen der Informationssysteme durch Schadsoftware (Näheres unter Kap. 16.1).

2.2 Die Geschäftsstelle während der Pandemie

Arbeiten in Zeiten einer Pandemie; eine vollkommen neue Erfahrung – auch für den Landesbeauftragten.

Der Landesbeauftragte wurde in der Pandemie wie alle anderen Behörden dieses Landes vor neue Herausforderungen gestellt, um die Aufgabenwahrnehmung auch in diesen besonderen Zeiten sicherzustellen.

Da wären zum einen die technischen Herausforderungen. Der Landesbeauftragte hat nicht zuletzt unter datenschutzrechtlichen Gesichtspunkten eine auf Abschottung von der Außenwelt ausgerichtete IT-Infrastruktur. Die elektronische Akte ist noch nicht eingeführt. Telearbeit ist nicht zuletzt deswegen in der Vergangenheit keine Form der Aufgabenerledigung beim Landesbeauftragten gewesen. Fragen der IT-Sicherheit wurden stets über die des Nutzungskomforts der IT-Systeme gestellt. Um am bestehenden Sicherheitsniveau festzuhalten, konnte und wollte der Landesbeauftragte – anders als in vielen anderen Behörden – nicht einfach Zugriff von außen auf seine Datenbestände gewähren. Er hat dennoch Lösungen gefunden, die datenschutzrechtlich vertretbar sind, um Arbeiten im häuslichen Umfeld zu ermöglichen. Darüber hinaus musste innerhalb kurzer Zeiträume die Teilnahme an und die Durchführung von Videokonferenzen ermöglicht werden. Von der Nutzung von Videokonferenzräumen anderer Behörden, über die provisorische Nutzung von Laptops hat sich der Landesbeauftragte zwischenzeitlich videokonferenztechnisch soweit ertüchtigt, dass er auf fast alle sich ergebenden Situationen angemessen reagieren kann. Das verlangte Investitionen in entsprechende Hardware, was sich jedoch bewährt hat. Technisch ist der Landesbeauftragte mit den Herausforderungen der Pandemie gut zurechtgekommen.

Die Pandemie hat allen Beteiligten diverse und sich ständig ändernde neue gesetzliche Regelungen beschert. Den Überblick zu behalten war und ist schwer; die Anforderungen an Arbeitgeber sind komplex. Der verwaltungstechnische Aufwand der Pandemie ist eine nicht zu unterschätzende Größe. Bei aller Schnelllebigkeit aufgrund ständig wechselnder Pandemielagen war es eine der größten Herausforderungen, die Rechtsordnung als Ganzes nicht aus dem Blick zu verlieren und dies auch zu kommunizieren. Der Landesbeauftragte musste in eigenen Angelegenheiten das vertretbare Maß finden mit der pandemiebedingten Sondersituation umzugehen. Alle zu Tage getretenen Facetten einzubinden und dennoch eine angemessene Aufgabenwahrnehmung sicherzustellen, war die Herausforderung des Jahres 2020.

2.3 Unzureichende Personalausstattung der Geschäftsstelle

In seinem XVI. Tätigkeitsbericht für das Jahr 2019 (Nr. 2.2) hat der Landesbeauftragte ausführlich dargestellt, wie die Personalausstattung eben nicht mit dem seit 2018 veränderten Aufgabenumfang mitgewachsen ist und dass vor allem der Umgang mit entsprechenden Anmeldungen zu den Haushaltsplänen durch das Ministerium der Finanzen des Landes Sachsen-Anhalt einen eklatanten Verstoß gegen die geltende Rechtslage und eine unzulässige Einflussnahme der Landesregierung auf die unabhängige Amtsausübung des Landesbeauftragten darstellt.

An der Gesamtsituation für den Landesbeauftragten hat sich seither nichts verändert. Der gutachterlich nachgewiesene Stellenbedarf besteht weiterhin, und dafür, dass die

Landesregierung im laufenden Haushaltsaufstellungsverfahren die rechtlichen Grenzen wahren wird, gibt es keinerlei Anzeichen.

An dieser Stelle soll dennoch nicht wiederholt werden, was bereits mehrfach dokumentiert wurde, sondern die Situation von der Seite der Auswirkungen her betrachtet werden.

Im Jahr 2018 ist das Arbeitsaufkommen für den Landesbeauftragten sprunghaft angestiegen; seither hält es sich auf diesem erhöhten Niveau mit zwar nicht mehr sprunghaften aber dennoch deutlichen Steigerungsraten. Zur Verdeutlichung wird auf eine Zahl aus dem Beitrag unter Nr. 3 dieses Tätigkeitsberichtes verwiesen. Die Steigerungsrate allein bei den Posteingängen beim Landesbeauftragten liegt im Vergleich zum „Vor-2018-Niveau“ bei über 100%. Dem steht ein prozentualer Stellenaufwuchs von 15% gegenüber, von dem die Hälfte dafür verwendet werden musste, die seit 2018 neue Eigenverwaltung der Geschäftsstelle in den Bereichen Organisation, Personal und Haushalt sicherzustellen. Demnach stehen 100% Steigerung des Arbeitsaufkommens bei der aufsichtsbehördlichen Tätigkeit 7,5% Stellenauswuchs für die aufsichtsbehördliche Tätigkeit gegenüber.

Die Gesamtsituation zwingt den Landesbeauftragten, Aufgaben in einer Art zu priorisieren, die bereits die Erfüllung seiner zwingenden gesetzlichen Verpflichtungen nicht mehr ermöglicht. So müssen Pflichtprüfungen zurückgestellt werden. Gesetzlich vorgesehene Höchstbearbeitungszeiten können nicht eingehalten werden. Darüber hinaus müssen auch genau die Aufgaben, die der Landesbeauftragte für die Bürgerinnen und Bürger dieses Landes sowie die Wirtschaftsunternehmen in diesem Land insbesondere wahrnehmen will, eingeschränkt werden. Der Landesbeauftragte kann fast ausschließlich reagieren. Für ein zielgerichtetes Agieren – vor allem im Interesse dieses Landes – bleibt praktisch kein Spielraum. Diese Einschränkung seiner Möglichkeiten mangels ausreichender personeller Ausstattung widerspricht nicht nur der Idee von einer Landesverwaltung, die für die Bürgerinnen und Bürger dieses Landes da ist. Sie widerspricht auch dem sich selbst erteilten gesetzlichen Auftrag aus § 22 Abs. 2 Satz 2 DSAG LSA, dem Landesbeauftragten die zur Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Das Land hat dem Landesbeauftragten 2018 umfangreiche und zusätzliche Aufgaben übertragen und sich gleichzeitig selbst verpflichtet, den Landesbeauftragten auch in personeller Hinsicht für die Wahrnehmung dieser Aufgaben auszustatten. Es gibt ein Gutachten und es gibt die Zahlen in diesem Tätigkeitsbericht (Nr. 3), die die derzeitige personelle Unterausstattung belegen.

2.4 Besonderes elektronisches Behördenpostfach

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

Das besondere elektronische Behördenpostfach (beBPo) ist ein E-Mail-ähnlicher Dienst, insbesondere für Behörden, der eine OSCI-basierte Verschlüsselung verwendet und die Komplexität des verschlüsselten elektronischen Datenaustauschs vor den Nutzern weitgehend verbirgt. § 6 ERVV sieht das beBPo unter anderem als sicheren Übermittlungsweg für die elektronische Kommunikation mit den Gerichten vor. Analog dazu gibt es für Anwälte das besondere elektronische Anwaltspostfach (beA) und für

Notare das besondere elektronische Notarpostfach (beN). Der Einsatz des beBPo beschränkt sich nicht nur auf die Kommunikation mit Gerichten; es kann auch durch Behörden für die Kommunikation untereinander verwendet werden. Bürger können u. U. als Nutzer der absenderbestätigten De-Mail an der sicheren Kommunikation teilnehmen.

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

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

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

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

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

---

[4] § 130a Zivilprozessordnung, § 46c Arbeitsgerichtsgesetz, § 65a Sozialgerichtsgesetz, § 55a Verwaltungsgerichtsordnung, § 52a Finanzgerichtsordnung, § 32a Strafprozessordnung, …

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

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

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

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

3 Entwicklung des Arbeitsaufkommens – Fallstatistik

In seinem XVI. Tätigkeitsbericht für das Jahr 2019 (Kap. 3) hat der Landesbeauftragte die Entwicklung der Anzahl der Posteingänge bei ihm für die Jahre 2016 bis 2019 dargestellt. Den Zahlen konnte eindeutig entnommen werden, dass mit der grundlegenden Änderung der Rechtslage durch das Inkrafttreten von Datenschutz-Grundverordnung und JI-Richtlinie im Jahr 2018 das Arbeitsaufkommen sprunghaft zugenommen hat. Die nunmehr nachfolgend dargestellten Zahlen bestätigen, dass sich das Arbeitsaufkommen weiterhin auf hohem Niveau eingependelt hat; trotz Corona-Pandemie.

Anzahl der registrierten Posteingänge

2016	5.506	
2017	6.737	
2018	9.602	zuzüglich 3.306 Meldungen gem. Art. 37 Abs. 7 DS-GVO

2019	10.941	zuzüglich 746 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2020	13.730	zuzüglich 764 Meldungen gem. Art. 37 Abs. 7 DS-GVO

Im Jahr des Inkrafttretens von Datenschutz-Grundverordnung und JI-Richtlinie lag die Steigerungsrate der registrierten Posteingänge bei 42%. Zwischenzeitlich liegt die Steigerungsrate gemessen an den Zahlen vor Änderung der Rechtslage bei über 100%. Selbst wenn nicht jeder Posteingang eine tiefergehende Befassung verlangt, zeigen die Zahlen dennoch sehr deutlich, dass der Landesbeauftragte dauerhaft ein stark erhöhtes Arbeitsaufkommen zu bewältigen hat.

Um für sich und ggf. auch für die interessierte Öffentlichkeit nachvollziehen zu können, worin Schwerpunkte der Tätigkeit des Landesbeauftragten liegen, führt er für wesentliche Bereiche eine Geschäftsstatistik. Innerbehördliche Angelegenheiten sind nicht erfasst, sodass sich ein klares Bild seiner Aufsichtstätigkeit erschließen lässt. Wesentliche aufsichtsbehördliche Aufgabenfelder werden nachfolgend dargestellt.

Beschwerden und Eingaben	452
Informations- und Beratungsfälle	1.282
Meldungen von Datenschutzverletzungen	216
Abhilfemaßnahmen/Anordnungen	28
Eingeleitete Bußgeldverfahren	17
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz)	17
Förmliche Begleitung von Rechtsetzungsvorhaben	27

Im Bereich der datenschutzaufsichtsbehördlichen Tätigkeit ist im Vergleich zum Jahr 2019 eine Steigerungsrate von 17% zu verzeichnen.

Wie die Zahlen zeigen, hat sich das Arbeitsaufkommen des Landesbeauftragten seit dem Inkrafttreten von Datenschutz-Grundverordnung und JI-Richtlinie im Jahr 2018 in einem erheblichen Ausmaß gesteigert. Vor diesem Hintergrund verwundert es, dass das Bedürfnis nach einer sachgerechten Personalausstattung wiederholt und jeweils ohne Aussprache mit dem Landesbeauftragten in Abrede gestellt wird.

4 Nationales und europäisches Datenschutzrecht

4.1 Fast drei Jahre Anwendung der Datenschutz-Grundverordnung

Zum Ende des Berichtszeitraums dieses Tätigkeitsberichts sind die DS-GVO und auch das neue Bundesdatenschutzgesetz bereits seit mehr als zweieinhalb Jahren anzuwenden. In dieser Zeit hat die DS-GVO viel Kritik erfahren. Laut einer Studie des Bitkom e. V.[5] hätte nach einer repräsentativen Befragung erst ein Viertel der Unternehmen die DS-GVO vollständig umgesetzt. 29% der Befragten hätten angegeben, dass die DS-GVO Innovationen verhindere. Fast drei Viertel der Befragten gaben an, dass Ihre Kunden von zusätzlichen Informationsblättern und Hinweisen genervt seien. Aus derselben Studie ergibt sich jedoch auch, dass zwei Drittel davon überzeugt sind, dass die DS-GVO weltweit Maßstäbe für den Umgang mit personenbezogenen Daten setzen wird; mehr als die Hälfte glaubt, dass sie zu einheitlicheren Wettbewerbsbedingungen in der EU führen wird.

Zugegeben: Die DS-GVO stellt hohe Anforderungen, insbesondere an die Erfüllung der Informations- und Dokumentationspflichten. Aber: der Aufwand ist begrenzt und lohnt sich.

Viele beim Landesbeauftragten eingegangene Beschwerden betroffener Personen zeigen, dass sie z. B. wissen wollen, welche Daten über sie aus welchen Gründen verarbeitet, insbesondere an wen sie übermittelt werden. Die Zunahme der Beschwerden gegenüber dem vorherigen Berichtszeitraum (vgl. Kap. 3) deutet auf eine aktivere Auseinandersetzung mit dem Datenschutz hin. Die Verarbeitung der eigenen personenbezogenen Daten wird sensibler wahrgenommen. Daher schafft die Erfüllung der Informationspflichten Vertrauen bei Geschäftspartnern und Beschäftigten. Im Rahmen der Beschwerdebearbeitung aber auch bei vielen Anfragen von Verantwortlichen wies der Landesbeauftragte auf Verfahren hin, wie die Informationspflichten durch einen möglichst geringen Verwaltungsaufwand erfüllt werden können.

Die Erfüllung der Dokumentationspflichten, vorwiegend das Führen des Verzeichnisses von Verarbeitungstätigkeiten, ermöglicht den Verantwortlichen die Überprüfung der Zulässigkeit der Verarbeitung personenbezogener Daten. Die Datenschutzkonferenz hat hier diverse Unterlagen bereitgestellt – z. B. einen Vordruck zum Erstellen des Verzeichnisses von Verarbeitungstätigkeiten – welche den Aufwand für die Unternehmen minimieren. Vor diesem Hintergrund dürfte das Führen des Verzeichnisses von Verarbeitungstätigkeiten auch für KMU eine mit überschaubarem Aufwand verbundene Aufgabe sein. Der Landesbeauftragte fordert bei schlüssigen Beschwerden oft das Verzeichnis an und erhält so einen mit wenig Einzelaufwand verbundenen Überblick über die gerügte Datenverarbeitung.

Fraglich ist allerdings, ob es dabei bleiben muss, dass die Verantwortlichen im Falle einer Datenschutzverletzung den Vorfall bei jedem Risiko melden müssen. Dies sieht zwar Art. 33 Abs. 1 DS-GVO vor, führt aber zu einer Fülle von Meldungen, die von den Aufsichtsbehörden aufgrund begrenzter Personalausstattung kaum detailliert geprüft werden können. Ohnehin müssten die Verantwortlichen selbst prüfen, wie sie die

[5] https://lsaurl.de/BitkomPM29092020

Rechtmäßigkeit und Sicherheit der Verarbeitung aufrechterhalten bzw. wiederherstellen. Im Rahmen einer zukünftigen Evaluierung der DS-GVO sollte daher erneut geprüft werden, ob es ausreicht, die Meldepflicht an das Erreichen einer bestimmten Risikoschwelle zu knüpfen (zur Evaluierung s. Nr. 4.3).

Verantwortliche – Unternehmen wie Behörden – setzen nach dem Eindruck des Landesbeauftragten die DS-GVO zunehmend um. Sie sind über grundsätzliche Vorgaben informiert und berücksichtigen sie. In Einzelfällen war die Datenverarbeitung allerdings mit teilweise erheblichen Mängeln behaftet, was zu Eingriffsmaßnahmen des Landesbeauftragten – mitunter auch zu Bußgeldverfahren – geführt hat. Grundlegende Kritik an der DS-GVO schwächt sich mit fortschreitender Zeit deutlich ab. Dies mag mit daran liegen, dass Gefahren, die angesichts der Geltung der DS-GVO befürchtet wurden, sich nicht realisiert haben. So ist z. B. die von Kritikern vorausgesagte große Abmahnwelle wegen Datenschutzverstößen ausgeblieben.

Insgesamt kann die DS-GVO aus Sicht des Landesbeauftragten als Erfolg betrachtet werden. Es sind zwar noch nicht alle Ziele erreicht. So führen insbesondere die vielen Öffnungsklauseln dazu, dass viele mitgliedstaatliche Sonderregelungen existieren. Gleichwohl wurde der Datenverkehr in der EU und im Europäischen Wirtschaftsraum deutlich erleichtert. Wesentlich ist, dass die DS-GVO die Rechte der betroffenen Personen deutlich gestärkt und der Schutz personenbezogener Daten in der öffentlichen Wahrnehmung einen höheren Stellenwert eingenommen hat.

Diese positiven Feststellungen treffen nicht nur für den nichtöffentlichen Bereich zu, sondern auch für die der DS-GVO unterliegenden öffentlichen Stellen im Land. Die vielfachen Anfragen aus öffentlichen Stellen zu einzelnen Aspekten der Umsetzung der DS-GVO und die Bitten um das Angebot von Schulungen haben dem Landesbeauftragten gezeigt, dass die Aufmerksamkeit gegenüber datenschutzrechtlichen Fragestellungen erheblich gestiegen ist. Die Erfahrung des Landesbeauftragten zeigt aber auch, dass mit den jeweils handelnden Personen vor Ort der Erfolg der Umsetzung datenschutzrechtlicher Vorschriften in der täglichen Praxis steht und fällt.

Die Kontakte des Landesbeauftragten mit den behördlichen Datenschutzbeauftragten verschiedener Einrichtungen (u. a. Oberste Landesbehörden, Hochschulen, Landkreise) wiesen auf eine stark gestiegene einrichtungsinterne Beratungstätigkeit hin. Auch wenn nun genauer hingeschaut wird und die einzelne Datenverarbeitung dadurch mehr Sorgfalt erfordert, führt die insgesamt spürbar gestiegene Sensibilität zu einem Gewinn in Bezug auf Rechtskonformität und Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger.

4.2 Parlament und Datenschutz-Grundverordnung

Im XV. Tätigkeitsbericht (Nr. 4.2) hatte der Landesbeauftragte die Frage der Anwendung der Datenschutz-Grundverordnung auf Parlamente, insbesondere die parlamentarische Kerntätigkeit, aufgegriffen. Der Beschluss der Datenschutzkonferenz wurde dargestellt, wonach auf Datenverarbeitungen von Parlamenten (auch von Fraktionen und Abgeordneten), die den parlamentarischen Kerntätigkeiten zuzuordnen sind, die DS-GVO keine Anwendung findet. Im XVI. Tätigkeitsbericht (Nr. 4.1.1) wurde zur Anpassung des Landesrechts auf die Ausgestaltung im DSAG LSA hingewiesen, wonach die DS-GVO für den Fall, dass sie nicht direkt auf den Landtag anwendbar wäre, entsprechend anzuwenden ist.

Nun hat der Europäische Gerichtshof für einen Petitionsausschuss eines Bundeslandes entschieden (EuGH, 9. Juli 2020, Az: C-272/19), dass dieser der Anwendung der DS-GVO unterliegt. Die Datenschutzkonferenz hat daraufhin den o. g. Beschluss zunächst ausgesetzt.[6] Die Begründung des EuGH lässt einerseits zumindest erkennen, dass das Gericht die DS-GVO auf die gesamte parlamentarische Tätigkeit für anwendbar hält. Andererseits wird im Wesentlichen mit der administrativen Natur der Tätigkeit des Petitionsausschusses argumentiert, was gegen eine Anwendung auf die legislative Tätigkeit spricht. § 3 Abs. 2 Nr. 3 DSAG LSA, wonach die DS-GVO auf nicht in den sachlichen Anwendungsbereich des Unionsrechts fallende Tätigkeiten entsprechende Anwendung findet, ist letztlich nicht betroffen, da dort keine spezifische Regelung enthalten ist. Geht man nach der Entscheidung des EuGH davon aus, dass Parlamente insgesamt der DS-GVO unterliegen, ist diese direkt anwendbar. Nur wenn dies, wie bisher angenommen, nicht der Fall wäre, würde die allgemein formulierte Regelung des § 3 Abs. 2 Nr. 3 DSAG LSA zur entsprechenden Anwendbarkeit führen.

4.3 Evaluierung der Datenschutz-Grundverordnung

Am 24. Juni 2020 veröffentlichte die EU-Kommission ihren gemäß Art. 97 Datenschutz-Grundverordnung (DS-GVO) erstellten Evaluierungsbericht. Die EU-Kommission zieht eine positive Zwischenbilanz der Anwendung und der Auswirkungen der DS-GVO und sieht ganz im Gegensatz zur Auffassung vieler deutscher Aufsichtsbehörden keinen Änderungsbedarf an den Vorschriften der DS-GVO. Zum Untersuchungsschwerpunkt „Zusammenarbeit und Kohärenz (Kapitel VII. DS-GVO)“ stellt die EU-Kommission fest, dass die Rechtsanwendung, insbesondere in der Zusammenarbeit der Aufsichtsbehörden, noch besser werden muss. Denn vor allem die Bearbeitung grenzüberschreitender Fälle erfordere einen effizienteren, einheitlicheren Ansatz und einen wirksamen Einsatz aller in der DS-GVO für die Zusammenarbeit der Datenschutzaufsichtsbehörden vorgesehenen Mechanismen. Es könne noch mehr für eine echte gemeinsame Datenschutzkultur getan werden.

Die Ausführungen der EU-Kommission sind als deutliche Kritik an der Arbeitsweise vornehmlich einiger weniger Aufsichtsbehörden zu verstehen, deren Aufgabe es ist, die großen amerikanischen Konzerne, die überwiegend ihre Geschäftsmodelle noch nicht vollständig an die europäischen Datenschutzvorschriften angepasst haben, zu beaufsichtigen. Das One-Stop-Shop-Prinzip der DS-GVO, wonach nur die Aufsichtsbehörde an der Hauptniederlassung des Unternehmens federführend zuständig ist, führt dazu, dass diese Aufsichtsbehörden trotz ihrer Pflicht zur Zusammenarbeit mit den anderen betroffenen Aufsichtsbehörden die Verfahren maßgeblich gestalten können.

Seit Mai 2018 ist trotz einer Vielzahl von Beschwerden und großem Druck von Seiten der anderen betroffenen Aufsichtsbehörden noch keine nennenswerte Zahl aufsichtsbehördlicher Entscheidungen gegenüber den großen US-Konzernen ergangen. Einige Aufsichtsbehörden haben es bislang verstanden, sich unter Berufung auf ihre Unabhängigkeit, das nationale Verwaltungsrecht und unter Nutzung von Unklarheiten bei der Auslegung von Vorschriften der DS-GVO einer effektiven Zusammenarbeit zu entziehen.

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

Über dem zweiten Evaluierungsschwerpunkt „Übermittlung von Daten in Drittländer, d. h. in Länder außerhalb der EU (Kapitel V. DS-GVO)“, schwebte das Damoklesschwert der EuGH-Entscheidung zu „Schrems II“ (vgl. Nr. 5.2). In Vorahnung eines wegweisenden Urteils stellte die EU-Kommission alle Instrumente des Datenexports und hier insbesondere ihre Angemessenheitsbeschlüsse sowie die ebenfalls von ihr erlassenen Standarddatenschutzklauseln unter einen Überarbeitungs- und Modernisierungsvorbehalt. In seinem Urteil vom 16. Juli 2020 nahm der EuGH dann tatsächlich die Gelegenheit wahr, das angemessene Schutzniveau zu beschreiben, das im Recht und der Praxis des Drittstaates gewährleistet sein muss, erklärte den EU-US-Privacy-Shield-Beschluss für ungültig und unterstrich die Verantwortung der Datenexporteure, nach einer einzelfallbezogenen Risikoanalyse die Instrumente des Datenexports notwendigenfalls mit zusätzlichen Maßnahmen zu flankieren oder – wenn dies nicht gelingt – den Datenexport einzustellen.

Die EU-Kommission war seitdem in der Pflicht, nicht nur möglichst zeitnah ein neues Abkommen mit den USA auszuhandeln, sondern auch alle bestehenden Angemessenheitsbeschlüsse zu überprüfen sowie die Standarddatenschutzklauseln zu überarbeiten.

4.4 Zentralisierung der Datenschutzaufsicht für den Markt

Ein Kernziel der DS-GVO ist die Vereinheitlichung des Datenschutzrechts und seiner Anwendung innerhalb der EU. Auf der Ebene der EU soll die Erreichung des Zieles durch den EDSA sichergestellt werden. Dieser stellt die einheitliche Anwendung der DS-GVO vor allem durch Leitlinien und sonstige Handreichungen sowie Entscheidungen in Einzelfällen sicher. Dazu kann er im Rahmen des in Art. 63 ff. DS-GVO beschriebenen Kohärenzverfahrens Stellungnahmen gegenüber den Aufsichtsbehörden abgeben (Art. 64 DS-GVO) oder in den Fällen des Art. 65 DS-GVO im Rahmen der Beilegung von Streitigkeiten unter den Aufsichtsbehörden diesen gegenüber verbindliche Beschlüsse erlassen. Diese Befugnis besteht gegenüber allen Aufsichtsbehörden in allen Mitgliedstaaten der EU.

Für Unternehmen, Vereine und andere nichtöffentliche Stellen sind in Deutschland grundsätzlich die Aufsichtsbehörden der Bundesländer zuständig. Es sei denn, es liegen besondere Zuständigkeiten vor. Eine solche besteht z. B. zugunsten des Bundesbeauftragten für den Datenschutz im Bereich der Telekommunikations- und Postdienstleistungen. Auch die Aufsicht über die Verarbeitung im Bereich der Kirchen und religiösen Vereinigungen oder zu journalistischen Zwecken unterliegt nicht den Aufsichtsbehörden der Bundesländer. Innerstaatlich ist damit eine Fülle von Aufsichtsbehörden zuständig.

Die unabhängigen Datenschutzaufsichtsbehörden haben sich in der Datenschutzkonferenz zusammengeschlossen. Diese hat es sich unter anderem zur Aufgabe gemacht, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen. Bei Abstimmungen gilt das Mehrheitsprinzip, Entschließungen zu datenschutzpolitischen Fragen erfordern eine Zweidrittelmehrheit.

Da die Aufsichtsbehörden zu einzelnen, die Privatwirtschaft betreffenden Fragen im Detail differierende Auffassungen vertraten, wurde die Frage aufgeworfen, ob die Datenschutzaufsicht für den Markt vereinheitlicht werden sollte. Bezug genommen wurde

dabei auf ein Gutachten der Datenethikkommission.[7] Darin wird zunächst festgestellt, dass sich in Einzelfragen Aussagen zu datenschutzrechtlichen Anforderungen und eine divergierende Vollzugspraxis beobachten lassen. Das föderale Miteinander der Datenschutzaufsichtsbehörden in Deutschland erreiche bisher keine ähnliche Verbindlichkeit und Einheitlichkeit wie die des EDSA auf europäischer Ebene (Seite 103 des Gutachtens). Nach Veröffentlichung des Gutachtens im Jahre 2019 wurde das Thema in der Wirtschaftsministerkonferenz behandelt. In der Beratung vom 30. November 2020 wurde der Beschluss gefasst, die Bundesregierung zu bitten, gemeinsam mit den Ländern und den Datenschutzaufsichtsbehörden die bestehenden Zuständigkeiten der Datenschutzaufsicht für den Markt auf praktische Durchführbarkeit sowie die für eine Verbesserung der Zusammenarbeit der Datenschutzaufsicht erforderlichen Gesetzesänderungen zu prüfen.

Dieser Prüfung steht der Landesbeauftragte offen gegenüber. Allerdings gibt es gewichtige Gründe, die gegen eine Zentralisierung der Datenschutzaufsicht für den Markt bei einer (Bundes-) Behörde sprechen:

1. Die DS-GVO ist in weiten Teilen von Unternehmen und Behörden gleichermaßen anzuwenden. Lediglich für einzelne Bereiche, z. B. bei der Datenverarbeitung durch die Behörden zum Zwecke der Strafverfolgung und der Gefahrenabwehr, gilt besonderes Datenschutzrecht. Nur durch die Zuständigkeit einer Landesbehörde für den öffentlichen und den nichtöffentlichen Bereich wird gewährleistet, dass die Datenverarbeitung in beiden Bereichen innerhalb des Landes nach einheitlichen Maßstäben bewertet wird. Die Wirtschaft in Sachsen-Anhalt hätte sicherlich kein Verständnis, wenn ihre Datenverarbeitung nach anderen Maßstäben bewertet würde, als die Datenverarbeitung durch die Behörden.

2. Auch Unternehmen müssen bei der Verarbeitung personenbezogener Daten Landesrecht berücksichtigen. Ein aktuelles Beispiel für Sachsen-Anhalt sind die Verordnungen über Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus. Diese Verordnungen haben insbesondere viele kleine Unternehmen verpflichtet, bestimmte Kundenkontaktdaten zu verarbeiten. Weitere Beispiele für Landesregelungen, die bei der Verarbeitung personenbezogener Daten zu beachten sind, sind das Krankenhausgesetz, das Glücksspielgesetz, das Spielbankgesetz oder das Wohnraumaufsichtsgesetz. Eine Bundesbehörde wird kaum in der Lage sein, hinsichtlich des in den 16 Bundesländern differierenden Landesrechts zu beraten und es durchzusetzen. Die Aufsichtsbehörden eines Bundeslandes verfügen hier schon allein aufgrund der Beteiligung im Gesetzgebungsverfahren über detaillierte Kenntnisse.

3. Die wirtschaftlichen Strukturen in den Bundesländern weisen erhebliche Unterschiede auf. So ist die Wirtschaft in Sachsen-Anhalt weniger von Konzernzentralen als vielmehr von kleinen und mittleren Unternehmen (KMU) geprägt. Allein die Größe eines Unternehmens kann sich erheblich auf die Anwendung datenschutzrechtlicher Vorschriften auswirken. Der Landesbeauftragte hat insbesondere die KMU durch Beratungen unterstützt. Darüber hinaus können durch die Aufsichtsbehörden in den Ländern gesellschaftliche und politische

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

Gegebenheiten vor Ort in die Arbeit einbezogen werden. In jüngster Vergangenheit war in Sachsen-Anhalt z. B. ein intensiver Austausch mit Organisationen wie dem Branchennetzwerk Cluster IT Mitteldeutschland e. V., dem Wirtschaftsrat sowie dem zuständigen Landesministerium im Rahmen der Digitalen Agenda gewährleistet. Dadurch konnten Aspekte des digitalen Fortschritts (auch beim E-Government) und des Datenschutzes sowie auch der Informationsfreiheit landesspezifisch zusammengeführt werden.

4. Die Datenschutzaufsicht durch die Bundesländer ermöglicht es, dezentral vor Ort tätig zu werden. So können Beratungen von Unternehmen – soweit erforderlich – in den Unternehmen durchgeführt werden. Damit kann detaillierter auf die konkrete Datenverarbeitung Bezug genommen und die Qualität der Beratung erhöht werden. Beratungsanfragen können auch in den Geschäftsräumen des Landesbeauftragten durchgeführt werden, was unzumutbare Anfahrtswege für die Unternehmen verhindert. Auch Kontrollen können – wenn sinnvoll – vor Ort durchgeführt werden. Dies ermöglicht z. B. die Bewertung der Datenverarbeitung aufgrund eigener Wahrnehmung, ohne auf mitunter fehlerhafte oder unvollständige und für die Unternehmen zeitintensive Stellungnahmen angewiesen zu sein. Vorträge, zu denen der Landesbeauftragte und seine Bediensteten regelmäßig durch Unternehmen eingeladen werden, können ohne längere Anfahrtswege vor Ort durchgeführt werden. Auch die Teilnahme an regionalen Arbeitskreisen und Netzwerken ist so gewährleistet. So nimmt der Landesbeauftragte an den Beratungen des Erfa-Kreises Sachsen-Anhalt, der Gesellschaft für Datenschutz und Datensicherheit sowie an weiteren Arbeitskreisen einzelner Branchen teil und führt eigenständig einen Arbeitskreis mit den für Sachsen-Anhalt zuständigen Wirtschaftskammern durch.

5. Soweit der Bund sein Gesetzgebungsrecht im Bereich des Datenschutzes auf Art. 74 Abs. 1 Nr. 11 GG stützt (konkurrierende Gesetzgebung auf dem Gebiet der Wirtschaft), ist eine Regelung, nach der die Zuständigkeit für die Datenschutzaufsicht im nichtöffentlichen Bereich beim Bund liegt, nicht erforderlich. Nach Artikel 72 Abs. 2 GG hat der Bund die Gesetzgebungskompetenz im Bereich des Rechts der Wirtschaft, „wenn und soweit die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich macht“. Dazu ist keine Zentralisierung der Datenschutzaufsicht erforderlich.

   Zur Verfolgung des DSK-Ziels der Vereinheitlichung der Anwendung des Datenschutzrechts finden regelmäßig Beratungen statt. Ergebnisse dieser Beratungen sind im Wesentlichen Veröffentlichungen zur Auslegung und Anwendung datenschutzrechtlicher Vorschriften. Dazu gehören z. B. sogenannte Kurzpapiere sowie weitere Orientierungshilfen, Empfehlungen und Positionierungen. Diese Veröffentlichungen wurden und werden auch zukünftig im Konsens verabschiedet und belegen die weitestgehend einheitliche Anwendung datenschutzrechtlicher Vorschriften durch die Aufsichtsbehörden. Unterschiedliche Auffassungen sind auf wenige Ausnahmefälle beschränkt und beruhen mitunter auf der föderalen Struktur und den unterschiedlichen Lebensverhältnissen in den Bundesländern, vornehmlich aber auf dem Umfang der erst seit kurzer Zeit anzuwendenden Vorschriften, aber auch auf differierender Rechtspre-

chung. Der Landesbeauftragte wird sich verstärkt dafür einsetzen, dass die Abstimmung unter den Aufsichtsbehörden innerhalb der DSK eine einheitliche und kohärente Anwendung des Datenschutzrechts gewährleistet. Überlegungen, die Entscheidungen der Datenschutzkonferenz verbindlicher zu gestalten, sodass eine noch stärkere Vereinheitlichung der Auslegung und Anwendung des Datenschutzrechts erreicht werden kann, steht der Landesbeauftragte offen gegenüber. Dies könnte z. B. durch eine entsprechende Regelung in einem Staatsvertrag erreicht werden.

Aus den genannten Gründen wird ersichtlich, dass die derzeitigen Zuständigkeiten bei der Datenschutzaufsicht im nichtöffentlichen Bereich sachgerecht sind und dem föderalen Bundesstaat praxisnah Ausdruck verleihen. Bei diesen Zuständigkeiten sollte es bleiben. Eine Möglichkeit, eine noch konsistentere Aufsichtspraxis in Deutschland zu erreichen, könnte ein Staatsvertrag zwischen dem Bund und den Ländern sein. Darin könnte geregelt werden, wie die DSK bei Wahrung der Unabhängigkeit zu einer verbindlichen Entscheidung kommt. Die DSK könnte damit nach dem Vorbild des EDSA gestärkt werden.

5 Weitere europäische und internationale Entwicklungen

5.1 Europäischer Datenschutzausschuss

Der EDSA war neben der Bewältigung der datenschutzrechtlichen Problemlagen der Pandemie (vgl. Kap. 13), dem Brexit (vgl. Nr. 5.4) und der Folgen des EuGH-Urteils „Schrems II“ (vgl. Nr. 5.2) unter anderem vordringlich mit der Überwindung der im Zuge des Evaluierungsprozesses der DS-GVO (vgl. Nr. 4.3) festgestellten Defizite hinsichtlich der Zusammenarbeit der Aufsichtsbehörden, auch mittels einer gemeinsamen und effizienteren Datenschutzkultur, beschäftigt.

Auf Initiative aus den Reihen der Aufsichtsbehörden beschloss das EDSA-Plenum einen sog. Aktionsplan, der in der Formulierung von Zielen, die bis Mai 2021 zu erreichen seien, in einer Priorisierung der Arbeit der Fachuntergruppen und einer weitergehenden Formulierung der Strategie des EDSA 2021-2023 bestand.

Die Formulierung kurzfristiger Ziele und der Priorisierungsvorschläge der Fachuntergruppen beinhaltete eine vorübergehende Schwerpunktverlagerung der Arbeit des EDSA mit dem Ziel der schnellen Klärung von Schlüsselfragen der Aufsichtsbehörden zur Beschwerdebearbeitung, Zusammenarbeit und Kohärenz.

Die Strategie des EDSA 2021-2023 definiert aufbauend auf vier Säulen die strategischen Ziele des Ausschusses, indem drei Schlüsselaktionen pro Säule zur Erreichung dieser Ziele festgelegt werden. Die vier Hauptsäulen der EDSA-Strategie und die darauf aufbauenden Schlüsselaktionen sind:

- die Förderung der Harmonisierung und Erleichterung der Einhaltung von Vorschriften (Leitlinien in zentralen Regelungsbereichen, Förderung von Verhaltensregeln und Zertifizierung, zielgruppenorientierte Handreichungen);

- die Unterstützung einer effektiven Durchsetzung und einer effizienten Zusammenarbeit zwischen den nationalen Aufsichtsbehörden (ständige Evaluierung

und Verbesserung der Kooperationsverfahren, Rahmenrichtlinie für koordiniertes aufsichtsbehördliches Handeln, Expertenunterstützungspool);

- ein grundrechtsorientierter Ansatz für neue Technologien (proaktives Begleiten der Einführung neuer Technologien, verstärkte Konzentration auf Rechenschaftspflichten der Verantwortlichen, Kooperation mit Verbraucher- und Wettbewerbsschützern) und

- die globale Dimension (Werbung für Transfertools, Internationale Zusammenarbeit mit Drittstaaten – abstrakt, aber auch in Einzelfällen).

Die Strategie wird auch durch ein Arbeitsprogramm umgesetzt, in dem die Maßnahmen des EDSA näher ausgeführt werden. Dieses Arbeitsprogramm ist Anfang 2021 verabschiedet worden.

Darüber hinaus hat der EDSA im Berichtszeitraum eine große Zahl von Leitlinien und Handreichungen erarbeitet. Hervorzuheben sind:

- Leitlinien 03/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte,

- Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679,

- Leitlinien 05/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DS-GVO (Teil 1),

- Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen,

- Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten,

- Leitlinien 06/2020 zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DS-GVO,

- Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, sowie

- Leitlinien 08/2020 über die gezielte Ansprache von Nutzern sozialer Medien.

5.2 Folgen des EuGH-Urteils “Schrems II” und Anforderungen an die Datenübermittlung in Drittländer

EuGH Schrems II / Task-Force „Supplementary Measures“

Am 16. Juli 2020 erging die lang erwartete Entscheidung des EuGH in Sachen „Schrems II“ zur Übermittlung von personenbezogenen Daten in die USA (Az. C-

311/18).[8] Der Entscheidung lag die Beschwerde des Österreichers Maximilian Schrems gegen Facebook Ireland Ltd. ursprünglich aus dem Jahr 2013 zugrunde, mit der sich Herr Schrems gegen den Datenexport und den Zugriff auf seine Daten durch US-Sicherheitsbehörden wandte. Facebook Ireland Ltd. hatte laufend personenbezogene Nutzerdaten an den Server der Facebook Inc. mit Sitz in den USA exportiert.

Facebook Ireland Ltd. berief sich zunächst auf den EU-KOM-Beschluss zu „Safe Harbor“ als Grundlage zur Übermittlung personenbezogener Daten an US-Unternehmen. Am 6. Oktober 2015 erklärte der EuGH in Sachen „Schrems I“ (Az. C-362/14, vgl. XII. Tätigkeitsbericht, Nr. 3.2.1) den EU-KOM-Beschluss zu „Safe Harbor“ für ungültig.

Anschließend stützte Facebook Ireland Ltd. den Datenexport in die USA auf Standarddatenschutzklauseln (EU-KOM-Beschluss 2010/87/EU) und den EU-KOM-Beschluss zum „EU-US-Privacy Shield“ als Nachfolgeregelung zu „Safe Harbor“ (Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der RL 95/46/EG über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, vgl. XIII./XIV. Tätigkeitsbericht, Nr. 3.2.1).

Mit dem „Schrems II“-Urteil des EuGH wurde nun auch der EU-KOM-Beschluss zum „EU-US Privacy Shield“ für ungültig erklärt. Das US-Recht biete im Vergleich zum EU-Recht kein im Wesentlichen gleichwertiges Schutzniveau, so das Gericht. Den US-Sicherheitsbehörden seien unbeschränkte Überwachungsbefugnisse eingeräumt. Den betroffenen Personen hingegen würden keinerlei Garantien für ihre Rechte gewährt. Zudem hätten betroffene Nicht-US-Bürger keinerlei gerichtliche Rechtsschutzmöglichkeiten gegenüber den US-Behörden. Das Gericht bezieht sich dabei u. a. auf die US-nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12333.[9]

Das „Schrems II“-Urteil hat erhebliche Auswirkungen auf den gesamten Datentransfer in die USA. Betroffen sind u. a. Cloud- und Messenger-Dienste. Es dürften keine personenbezogenen Daten mehr auf Grundlage des „EU-US Privacy Shields“ übermittelt werden. Offen geblieben im Urteil ist die Frage, mit welchen Sicherheitsgarantien und Zusatzmaßnahmen Daten exportiert werden können, um dem *EU-Schutzniveau im Wesentlichen* zu entsprechen.

Grundsätzlich können für einen Datenexport Standarddatenschutzklauseln (Standard Contractual Clauses – SCC) und auch verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) genutzt werden, wenn die Datenverarbeitungen beim Empfänger im Drittland einem angemessenen Datenschutzniveau entsprechen. Die Risiken des Übertragungswegs und die Risiken, die sich aus der Speicherung der Daten bei einem spezifischen Empfänger (Zwang zur Kooperation mit Geheimdiensten) ergeben, müssen vorab durch den Verantwortlichen beurteilt werden. Das schließt auch die Erwägung zumutbarer Alternativen wie beispielsweise geeignete Anbieter in

[8] https://lsaurl.de/EuGHSchrems2

[9] https://lsaurl.de/DSKSchrems2

der EU mit ein, sodass kein Datentransfer in ein Drittland notwendig wird. Am 12. November 2020 legte die EU-Kommission den Entwurf neuer Standarddatenschutzklauseln vor. Der endgültige Beschluss erfolgte am 4. Juni 2021.[10]

Ergänzend zu den Standarddatenschutzklauseln verabschiedete der EDSA am 10. November 2020 zwei Dokumente (1/2020 und 2/2020), die die Verantwortlichen bei der Gestaltung datenschutzkonformer Datenexporte unterstützen sollen. Während die Empfehlungen 01/2020[11] zu Maßnahmen zur Ergänzung von Übermittlungsinstrumenten zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vorzunehmende Prüfschritte beschreiben, fassen die Empfehlungen 02/2020[12] zu den wesentlichen Garantien bei Überwachungsmaßnahmen zusammen, welche datenschutzrechtlichen Anforderungen an die Rechtsordnung eines Drittlandes zu stellen sind. Dort genannte wesentliche Garantien sind unter anderem Gegenstand der Prüfung, ob das Recht oder die Praxis des Drittlandes im Zusammenhang mit einer spezifischen Datenübermittlung irgendwelche Elemente enthält, die die Wirksamkeit des Übermittlungsinstruments, auf die sie sich stützt, beeinträchtigen könnten.

Die Empfehlungen 01/2020 wurden nach öffentlicher Konsultation am 18. Juni 2021 in überarbeiteter Version (2.0) verabschiedet.[13] Neuerungen ergeben sich bei den Pflichten zur Bewertung der Rechtslage des Drittlandes im Sinne eines angemessenen Datenschutzniveaus. Nunmehr dürfen die „praktischen Erfahrungen“ des Empfängers mit Herausgabeersuchen oder Abgriffen durch (Sicherheits-)Behörden in die Bewertung mit einfließen.

Im Zuständigkeitsbereich des Landesbeauftragten gibt es eine Vielzahl von Verantwortlichen, die von dem Urteil unmittelbar oder mittelbar betroffen sind. Unternehmer und öffentliche Stellen sind aufgerufen, ihre Verfahren zum Datentransfer anhand des Urteils des EuGH und den o. g. Empfehlungen des EDSA zu überprüfen und ggf. entsprechend anzupassen. Viele Unternehmen nutzen „Tracking-Tools“ auf ihren Webseiten. Derzeit wird hier davon ausgegangen, dass eine gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) mit dem Anbieter des Tools zumindest in der Phase der Erhebung und Übermittlung an den Anbieter des Tools besteht, sofern dieser die Daten auch zu eigenen Zwecken verarbeitet. Anlassbezogen werden Unternehmen wegen des möglichen Datenexports in die USA vom Landesbeauftragten befragt und beraten.

Infolge des o. g. „Schrems II“-Urteils erhob im August die Organisation NOYB (My Privacy is „None of Your Business“) 101 Beschwerden gegen europäische Unternehmen, die die Dienste Google Analytics oder Facebook Connect auf ihren Webseiten einbinden. Inhaltlich ist fraglich, ob Google und Facebook über die genannten Produkte personenbezogene Daten in die USA übermitteln dürfen. Beide Konzerne stützen sich auf Standarddatenschutzklauseln. Ob ausreichende zusätzliche Maßnahmen getroffen wurden, um dem *EU-Schutzniveau im Wesentlichen* zu entsprechen (s. o.), ist von den zuständigen nationalen Aufsichtsbehörden zu klären. Der EDSA richtete die Task

[10] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=de

[11] https://lsaurl.de/EDSA012020

[12] https://lsaurl.de/EDSA022020

[13] https://lsaurl.de/EDSA012020v2

Force „101“ ein, die die Aufsichtsbehörden unterstützen und auf eine einheitliche Bewertung hinwirken soll.

5.3 Das neue BCR-Verfahren und die nationale Umsetzung verbindlicher interner Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“, BCR) eines Unternehmens bzw. Konzerns erlauben es, personenbezogene Daten an eine verbundene Stelle bzw. an ein Unternehmen des Konzerns in einem Drittland zu übermitteln, selbst wenn das Drittland nicht über ein der EU vergleichbares Schutzniveau verfügt. Voraussetzung ist aber, dass die BCR geeignete Garantien für den Schutz von personenbezogenen Daten im Sinne des Art. 46 Abs. 1 und 2 lit. b DS-GVO bieten und die zuständige Aufsichtsbehörde die BCR nach einem formellen Kohärenzverfahren nach Art. 47 Abs. 1, Art. 63 DS-GVO genehmigt hat. In dem Verfahren gibt der EDSA eine Stellungnahme zur beabsichtigten Genehmigung ab (Art. 64 Abs. 1 lit. f DS-GVO). Der EDSA schaltet nunmehr dem Kohärenzverfahren mit dem sog. „BCR Session Meeting“ ein informelles Verfahren als weitere Abstimmungsrunde vor. Neben der zuständigen (federführenden) Aufsichtsbehörde können sich alle europäischen Aufsichtsbehörden daran beteiligen. Auf nationaler Ebene wurde diskutiert, ob sich deutsche Aufsichtsbehörden beteiligen sollten, wenn das betreffende Unternehmen keine Hauptniederlassung in Deutschland hat. Der Landesbeauftragte schlug in der 99. DSK vor, dass eine deutsche Aufsichtsbehörde obligatorisch eine BCR (mit-)prüft, wenn in ihrem örtlichen Zuständigkeitsbereich das Unternehmen seinen deutschen Hauptsitz hat. Verfügt das Unternehmen dagegen über keine deutsche Niederlassung, können alle deutschen Aufsichtsbehörden BCR mitprüfen und fungieren dann als deutsche Berichterstatter im „BCR Session Meeting“. Die DSK beschloss, dass die deutschen Aufsichtsbehörden jedoch in diesem Fall keine Prüfobliegenheit trifft.

Vor dem Hintergrund der EuGH-Entscheidung in Sachen „Schrems II“ (s. Nr. 5.2) müssen auch BCR so angepasst werden, dass der Datentransfer in ein Drittland ggf. unter dem Einsatz zusätzlicher Maßnahmen dem *EU-Schutzniveau im Wesentlichen* entspricht.

5.4 Brexit

In seinem XVI. Tätigkeitsbericht (Nr. 5.3) hatte der Landesbeauftragte bereits zu der Einigung zwischen der Europäischen Union und dem Vereinigten Königreich (UK) auf das Austrittabkommen am 14. November 2018 und der darin vorgesehenen Übergangsphase bis voraussichtlich 31. Dezember 2020 berichtet, nach der das Vereinigte Königreich zunächst wie bisher alle EU-Regeln einhält und weiterhin Beiträge zahlen wird, aber in EU-Gremien keine Mitsprache mehr hat. Die langfristigen Beziehungen zwischen dem Vereinigten Königreich und der EU wurden in 2020 dann Gegenstand weiterer Verhandlungen.

In den Schlussbestimmungen des erst Ende 2020 ausverhandelten Handels- und Zusammenarbeitsabkommens (Trade and Cooperation Agreement, TCA) zwischen der Europäischen Union und dem Vereinigten Königreich (Article 10A Interim provision for transmission of personal data to the United Kingdom, S. 406 ff.) war nunmehr eine neue Übergangsregelung für Datenübermittlungen vorgesehen. Die Geltung der Übergangsregelung war an eine Reihe von Voraussetzungen geknüpft. So durfte das Vereinigte Königreich seine Datenschutzgesetze (Data Protection Act 2018 und auf UK

„angepasste DS-GVO“) nicht ändern und keine Handlungen ausüben, die das aktuelle Datenschutzniveau abändern.

Damit konnten die Befürchtungen eines sog. ungeregelten Austritts des Vereinigten Königreichs aus der Europäischen Union und die damit verbundene Konsequenz, das Vereinigte Königreich mit Blick auf Datenübermittlungen als Drittland anzusehen, zunächst abgewendet werden.

Für bereits bis zum 31. Dezember 2020 im Vereinigten Königreich gesammelte personenbezogene Daten („legacy data“) galt die DS-GVO eingefroren weiter, sie wurde daher auch als „frozen GDPR“ bezeichnet.

Danach sollten Übermittlungen personenbezogener Daten aus der Europäischen Union an Verantwortliche und Auftragsverarbeiter im Vereinigten Königreich und Nordirland für eine Übergangsperiode von letztlich sechs Monaten nicht als Übermittlungen in ein Drittland (Art. 44 DS-GVO) angesehen werden. Diese Periode begann mit dem In-Kraft-Treten des Abkommens am 1. Januar 2021.

Zwischenzeitlich hat die EU-Kommission zwei UK betreffende Angemessenheitsentscheidungen nach Art. 45 Abs. 3 DS-GVO und Art. 36 Abs. 3 JI-Richtlinie erlassen (28. Juni 2021, C(2021) 4800 final). Demnach gilt UK datenschutzrechtlich weitestgehend als „sicheres Drittland“, d. h. bis auf Weiteres ist der Datenverkehr von Unternehmen aus Sachsen-Anhalt mit UK-Partnern ohne zusätzliche Erschwernisse möglich. Es besteht keine Notwendigkeit aufwendiger individueller Datensicherheitsgarantien für Datentransfers. Der Angemessenheitsbeschluss behält seine Gültigkeit vorerst bis zum 27. Juni 2025. Zum Ablauf dieses Zeitraums muss die EU-Kommission selbstständig neu prüfen, ob die Angemessenheit des UK-Datenschutzniveaus auch weiterhin gewährleistet ist.

Die verbleibenden europäischen Aufsichtsbehörden hatten verschiedene Folgeprobleme des Brexits zu bewältigen, denn zum Ende des Jahres 2020 ist die Datenschutzaufsichtsbehörde des Vereinigten Königreichs (Information Commissioner‘s Office, ICO) aus dem Verbund der Datenschutzaufsichtsbehörden der Europäischen Union ausgetreten.

Die nach Art. 47 Abs. 1 DS-GVO erforderlichen, bereits erteilten Genehmigungen von Binding Corporate Rules, bei denen UK als federführende Aufsichtsbehörde fungierte, wirkten nach dem Ende der Übergangszeit nicht fort (Infonote des EDSA vom 22. Juli 2020). Daher musste eine neue federführende Aufsichtsbehörde die Genehmigung nach dem Austritt und dem Ende der Übergangszeit neu erteilen. Der Findungsprozess der neuen federführenden Aufsichtsbehörden ist zeitnah abgeschlossen worden, hieran hatten vor allem die betroffenen Unternehmen ein großes Interesse.

Darüber hinaus mussten die noch offenen Beschwerden des One-stop-shop-Verfahrens, für die UK federführend zuständig war, von einer neuen federführend zuständigen Aufsichtsbehörde übernommen werden. Die Suche nach einer neuen Federführung oblag der Behörde, bei der die Beschwerde ursprünglich eingegangen war. UK hatte angeboten, auch nach der Übergangsphase in grenzüberschreitenden Fällen weiterhin mitzuarbeiten. Nach Rückfrage bei der EU-Kommission musste der EDSA dieses Angebot ablehnen (Infonote und Antwortbrief des EDSA vom 20. Oktober 2020). Eine Teilnahme der ICO an entsprechenden Sitzungen der Fachuntergruppen

des EDSA könne nur ausnahmsweise gestattet werden, eine andere Verfahrensweise verstieße gegen das Austrittsabkommen.

5.5 Europäischer Datenschutztag

Der Europäische Datenschutztag wird seit 2007 auf Initiative des Europarates alljährlich am 28. Januar begangen und nimmt damit Bezug auf die ursprüngliche Europaratskonvention 108 zum Datenschutz, genauer auf das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", das am 28. Januar 1981 zur Unterzeichnung aufgelegt wurde. Zur Europaratskonvention und ihrer Überarbeitung hatte der Landesbeauftragte bereits in seinem XVI. Tätigkeitsbericht (Nr. 5.4) berichtet. Seit dem 18. November 2020 bis zum 21. Mai 2021 hat Deutschland den Vorsitz im Ministerkomitee des Europarats inne.

An diesem Aktionstag für den Datenschutz sollen die Bürger Europas durch datenschutzspezifische Veranstaltungen von Behörden, Unternehmen und anderen Einrichtungen des gesellschaftlichen Lebens für den Datenschutz sensibilisiert werden.

Im Jahr 2020 lag das Augenmerk der Veranstaltung in Deutschland, insbesondere auf Datenschutz im Kontext des Entwicklungsfortschritts der KI. Unter dem Motto „Künstliche Intelligenz – Zwischen Bändigung und Förderung" wurden Freiheiten, Grundrechte und Schutzbedürfnisse bei der Schaffung von Rahmenbedingungen und der Entfaltung diesbezüglicher Aktivitäten von Referenten aus Politik, Wissenschaft und Recht sowie den Teilnehmern thematisiert.

Die Vorträge beschäftigten sich unter anderem mit den Themen „Aspekte des Unionsrechts im Hinblick auf Digitalisierung und Datenschutz", „Der Handlungsrahmen für KI-Anwendungen: Wirtschaft, Technik, Ethik und (Datenschutz-)Recht in Deutschland, Europa und der Welt" und „Was verstehen Nutzer unter Algorithmen?".

Im Rahmen der Podiumsdiskussion diskutierten Vertreter von Forschung und Lehre mit einem Vertreter der EU-Kommission zum Thema „Nutzen und Schaden von KI für den Einzelnen – Was geht mich KI an?"

5.6 Internationale Datenschutzkonferenz

Die 42. Internationale Datenschutzkonferenz (Global Privacy Assembly, GPA) fand vom 13. bis 15. Oktober 2020 mit mehr als 100 Vertretern pandemiebedingt als reine Online-Veranstaltung statt und stand unter dem Motto der „Erhöhung der internationalen Datenschutzstandards durch eine moderne, kollaborative globale Gemeinschaft".

Ziel war hier die weitere Modernisierung der GPA im Hinblick auf neue Wege zur Partnerschaft bzw. Zusammenarbeit, insbesondere mit wichtigen internationalen Organisationen wie der OECD bis hin zur Zusammenarbeit mit Tech-Unternehmen zum Datenschutz durch Design.

Die Konferenz verabschiedete verschiedene Entschließungen, u. a. zum Datenschutz und seinen Herausforderungen durch die COVID-19-Pandemie. Hier fordert die GPA beispielsweise datenschutzfreundliche Voreinstellungen bei der Kontaktnachverfolgung.

In einer weiteren Entschließung zur Beachtung der datenschutzrechtlichen Vorgaben bei der Entwicklung und Nutzung künstlicher Intelligenz (KI) wird die transparente und diskriminierungsfreie Verarbeitung personenbezogener Daten durch KI-Systeme gefordert.

In ähnlicher Weise werden im Rahmen der Entschließung zur Technologie der Gesichtserkennung die Gefahren der damit verbundenen starken Beeinträchtigung der Privatsphäre und der Diskriminierung deutlich gemacht.

Schließlich hat die GPA auch eine Entschließung zum Verfahren für die Verabschiedung gemeinsamer Erklärungen zu neuen globalen Fragen angenommen. Die GPA wird danach zukünftig auch außerhalb der Konferenz gemeinsame Stellungnahmen zu wichtigen globalen Datenschutzthemen veröffentlichen und damit viel besser in der Lage sein, zu aktuellen Themen sehr zeitnah reagieren zu können.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, wurde zudem einstimmig in das Leitungsgremium (Executive Committee) der Internationalen Datenschutzkonferenz gewählt. Er ist der erste deutsche Datenschutzbeauftragte, der diesem Gremium angehört, dessen Mitglieder für zwei Jahre bestimmt und einmalig wiedergewählt werden können.

Weiterführende Informationen finden sich auf der Webseite der GPA.[14] Das Angebot steht nur in englischer Sprache zur Verfügung.

6 Technik und Organisation

6.1 E-Government-Gesetz Sachsen-Anhalt

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

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

[14] https://globalprivacyassembly.org/

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

6.2 Onlinezugangsgesetz und Portalverbund

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

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

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

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

Unter datenschutzrechtlichen Gesichtspunkten ist zunächst darauf hinzuweisen, dass die Datenschutzaufsichtsbehörden des Bundes und der Länder keine Projektbeteiligten an den einzelnen Digitalisierungsvorhaben sind. Die Aufsichtsbehörden werden auch nicht als Genehmigungsbehörden tätig, die das Vorhaben für das jeweilige Land oder gar bundesweit per Verwaltungsakt datenschutzrechtlich genehmigen könnten. Es ist vielmehr Aufgabe des jeweiligen Landes bzw. des zuständigen Fachressorts,

eigenverantwortlich die Vereinbarkeit des Vorhabens mit den einschlägigen datenschutzrechtlichen Vorschriften zu prüfen. Die Datenschutzaufsichtsbehörden können dabei, wenn die Fachressorts die entsprechenden Vorarbeiten geleistet haben, beratend und unterstützend tätig werden.

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

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

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

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

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

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

Der Bund hat die oben dargestellte Problematik mittlerweile gesehen und in §§ 9a bis c E-Government-Gesetz des Bundes auf Bundesebene das Antragsportal und die datenschutzrechtliche Verantwortlichkeit gesetzlich geregelt. Eine Lösung auf Landesebene könnte darin bestehen, entsprechende Regelungen in das E-Government-Gesetz des Landes aufzunehmen.

Sinnvoll könnte es auch sein, in die Landesdatenschutzgesetze eine Befugnis zur Erhebung personenbezogener Daten und deren Übermittlung an die zuständige Behörde durch einen digitalen Antragsassistenten für die o. g. länderübergreifenden Fälle aufzunehmen. Vorbild für eine solche Regelung könnte z. B. § 24b Abs. 1 Satz 1 Bundeselterngeld- und Elternzeitgesetz sein.

Der Landesbeauftragte wird über die Ergebnisse der UAG weiter berichten.

6.2.1 BAföG Digital

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

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

Das Ministerium hält die Datenverarbeitung durch den Antragsassistenten gem. Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 4 Satz 1 Nr. 2 DSAG LSA für zulässig (erforderlich zur Erfüllung einer in der Zuständigkeit des Verantwortlichen liegenden Aufgabe, deren

Wahrnehmung im öffentlichen Interesse liegt). Nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO könne der Verantwortliche durch Recht der Mitgliedstaaten vorgegeben werden. Dies seien Normen, die eine Rechtspflicht im mitgliedstaatlichen Recht begründen. Verwaltungsvorschriften und auch die vorgenannte Verwaltungsvereinbarung wären insoweit ausreichend.

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

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

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

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

6.3 Verwaltungs- und Registermodernisierung – datenschutzkonform gestalten

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

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

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

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

Darin weist sie darauf hin, dass die Steueridentifikationsnummer bisher nur deswegen als verfassungskonform angesehen wird, weil sie einer engen Zweckbindung für steuerliche Zwecke unterliegt. Weiterhin attestiert die DSK ein hohes Missbrauchspotential in diesem sektorübergreifenden Ordnungsmerkmal, welches Bürgerdaten aus mehr als 50 Registern miteinander verknüpft und somit die technische und logische Grundlage dafür schafft, über weitere Gesetze verfassungsrechtliche Grundsätze aufzuweichen und eine zukünftige staatliche Profilbildung komplexer bürgerlicher Lebensverhältnisse zu ermöglichen. Auch kommt sie zu dem Schluss, dass die von autorisierten Behörden einsehbare Ende-zu-Ende-Verschlüsselung letztlich nicht vor einer missbräuchlichen Zusammenführung der Daten oder unbeabsichtigten Datenlecks schützen kann. Schließlich konstatiert sie, dass die Beschleunigung der Digitalisierung nicht als Argument benutzt werden darf, verfassungsrechtlich notwendige Nachbesserungen unter den Tisch fallen zu lassen.

Trotz der medienwirksamen Äußerung vorgenannter Kritikpunkte wurde der Entwurf zum RegMoG am 28. Januar 2021 vom Bundestag angenommen. Daraufhin wendeten sich die Datenschutzaufsichtsbehörden an die jeweils in ihren Ländern zuständigen Innenressorts und in einer gemeinsamen Pressemitteilung nochmals an Öffentlichkeit und Regierungen. Leider erfolglos, denn am 5. März 2021 stimmte der Bundesrat dem RegMoG zu. Die Einführung der Identifikationsnummer steht noch aus.

6.4 Dataport-Staatsvertrag

Seit dem Beitritt zum Staatsvertrag über die Errichtung von Dataport als rechtsfähiger Anstalt des öffentlichen Rechts 2013 gehört das Land Sachsen-Anhalt neben Schleswig-Holstein, Hamburg, Mecklenburg-Vorpommern, Bremen und Niedersachsen zu den Dataport-Trägerländern. Dataport erbringt seitdem für Sachsen-Anhalt für die öffentlichen Verwaltungen, einschließlich der Kommunalverwaltungen, eine Reihe von Leistungen auf dem Gebiet der Informations- und Kommunikationstechniken.

Aufgrund geänderter rechtlicher Rahmenbedingungen sind Anpassungen dieses Staatsvertrages notwendig geworden. Zu diesen geänderten Bedingungen sind vor allem die Umsetzung der DS-GVO und der jeweils angepassten Datenschutzgesetze der Trägerländer zu zählen. Darüber hinaus galt es, Zuständigkeiten und Regelungen anzupassen, um auch gemeinsame IT-Verfahren zu ermöglichen. Damit wurde eine trägerübergreifende einheitliche Rechtsgrundlage für den Betrieb von Abrufverfahren und gemeinsame Verfahren geschaffen. Der Landesbeauftragte hat den Änderungsprozess begleitet.

Mit der Änderung des Dataport-Staatsvertrags wird auch der gesetzliche Auftrag zur Unterstützung der öffentlichen Verwaltung der Trägerländer mit Informations- und Kommunikationstechniken festgeschrieben. Der Vertrag in der Fassung vom 29. November 2019 ist am 24. Juli 2020 in Kraft getreten.

6.5 Standard-Datenschutzmodell

Das Standard-Datenschutzmodell (SDM) ist eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Zuletzt wurde im XVI. Tätigkeitsbericht des Landesbeauftragten (Nr. 6.4) über die Veröffentlichung der überarbeiteten Fassung 2.0a berichtet. Diese wurde im April 2020 von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit wenigen redaktionellen Änderungen und unter Aufnahme von zusätzlichen Hinweisen zur Verbindlichkeit der Anwendung einzelner Maßnahmen des Maßnahmenkatalogs (Kap. E6) in der Version 2.0b verabschiedet.

Im SDM werden geeignete Mechanismen aufgezeigt, mit deren Hilfe die umfangreichen abstrakten datenschutzrechtlichen Anforderungen aus der DS-GVO in konkrete technische und organisatorische Maßnahmen überführt werden können. Dazu werden die Anforderungen systematisch Gewährleistungszielen des SDM zugeordnet. Diese beinhalten die klassischen Ziele der IT-Sicherheit – Vertraulichkeit, Verfügbarkeit, Integrität – und ergänzen sie um die weiteren datenschutzbezogenen Schutzziele Datenminimierung, Transparenz, Nichtverkettung und Intervenierbarkeit. Für alle relevanten Komponenten einer Datenverarbeitung, das sind Daten, Systeme und Dienste sowie Prozesse, werden für jedes der Gewährleistungsziele Referenzmaßnahmen ab-

geleitet. Diese sind im Referenzmaßnahmen-Katalog des SDM beschrieben. Zusätzlich sind in einer abschließenden Risikoanalyse noch ggf. darüber hinaus gehende Sicherungsbedarfe zu ermitteln. Eine dauerhaft korrekte und ausreichende Umsetzung ist zudem nur mit Implementierung eines Datenschutzmanagementprozesses zu gewährleisten. Dieser wird ebenfalls im SDM-Handbuch beschrieben und hilft Verantwortlichen dabei, alle Phasen der Verarbeitung personenbezogener Daten dauerhaft zu betrachten und eine rechtssichere Verarbeitung kontinuierlich zu gewährleisten (PDCA-Zyklus).

Die Entwicklung des Katalogs mit den konkreten standardisierten Schutzmaßnahmen setzt sich stetig fort. Im Jahr 2020 lag der Schwerpunkt auf der Erarbeitung einzelner Bausteine des Referenzmaßnahmen-Katalogs gemäß dem „Betriebskonzept für SDM-Bausteine“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der DSK.

Da die SDM-Gewährleistungsziele von grundrechtlichen Anforderungen abgeleitet sind, dient das SDM primär dem Schutz der Betroffenen bei der Verarbeitung personenbezogener Daten, während der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik die IT-Sicherheit, beispielsweise von Geschäftsprozessen, im Blick hat. Beide, das SDM und der IT-Grundschutz (mit dem Baustein CON.2 Datenschutz), ergänzen und bedingen einander in harmonischer und symbiotischer Weise.

Erfreulicherweise gab es im Berichtszeitraum und auch später einige Nachfragen von potenziellen Nutzerinnen und Nutzern zum SDM. Die jeweils letzte Fassung des Standard-Datenschutzmodells nebst den bereits veröffentlichten und vom AK Technik zur Anwendung „freigegebenen“ Bausteinen des SDM-Maßnahmenkatalogs sind auf den Webseiten des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zu finden.[15]

6.6 Akkreditierung und Zertifizierung

In den Art. 42 und 43 DS-GVO werden einheitliche Zertifizierungs- und Akkreditierungsverfahren geregelt. Eine solche Zertifizierung kann Produkte, Dienstleistungen oder Prozesse abdecken und dient dem Nachweis, dass personenbezogene Daten DS-GVO-konform verarbeitet werden. Die Vorlage eines Zertifikats schafft Vertrauen, das vorgegebene Anforderungen und Kriterien erfüllt werden, aber auch, dass ein Qualitätsniveau vorhanden ist, erhalten bleibt und sich idealerweise stetig verbessert. Sie kann entscheidender Wettbewerbsfaktor sein, aber auch nur dem Nachweis der Erfüllung der datenschutzrechtlichen Rechenschaftspflichten dienen. Eine erfolgreich durchgeführte Zertifizierung befreit eine Organisation nicht von der Verantwortung, die DS-GVO einzuhalten, sie kann jedoch bei aufsichtsbehördlichen Kontrollen positiv einfließen, die Prüfung etwa verkürzen oder vereinfachen.

Der Landesbeauftragte informierte in seinem XVI. Tätigkeitsbericht (Nr. 6.6) über die generelle Möglichkeit einer Zertifizierung, deren rudimentäre Abläufe und die Rolle der Deutschen Akkreditierungsstelle GmbH (DAkkS).

[15] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Stellen, die DS-GVO-konforme Datenschutzzertifizierungen vornehmen wollen, müssen zuvor akkreditiert werden. Die Akkreditierung ist durch die jeweils zuständige Aufsichtsbehörde vorzunehmen (Art. 57 Abs. 1 lit. q DS-GVO). Sie erfolgt in Deutschland zwar durch die DAkkS (Ausnahme nach Art. 41 Abs. 1 DS-GVO), diese greift jedoch auf die fachlichen Kompetenzen der jeweils zuständigen Aufsichtsbehörde zurück. Aufsichtsbehörden sind als Gutachter in die Entscheidungsfindung zur Akkreditierung eingebunden. Grundlage der Prüfung (Art. 43 Abs. 1 lit. b DS-GVO) ist die Norm EN-ISO/IEC 17065/2012 „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“, deren Anforderungen – etwa an Kompetenzen oder die Unparteilichkeit der Zertifizierungsstelle – erfüllt werden müssen. Weitere Anforderungen – nämlich zum Nachweis der Datenschutzkonformität – wurden in einem die Norm ergänzenden Dokument „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“ erfasst. Diese Kriterien für die Akkreditierung von Zertifizierungsstellen wurden zusammen mit den anderen deutschen Datenschutzaufsichtsbehörden erstellt und auch mit dem Europäischen Datenschutzausschuss (EDSA) abgestimmt (Art. 42 Abs. 5 i. V. m. Art. 64 Abs. 1 lit. c DS-GVO). Enthalten sind beispielhaft Anforderungen an die Fachkunde des Personals der Zertifizierungsstellen, zur Veröffentlichung von Dokumenten aber auch rechtliche und vertragliche Anforderungen.

Die Befugnis, als Zertifizierungsstelle tätig zu werden, wird gem. § 39 BDSG durch die zuständige Aufsichtsbehörde des Bundes oder der Länder erteilt. Nach einer erfolgreichen Akkreditierung können Zertifizierungsstellen dann eine Datenschutzzertifizierung nach der DS-GVO erteilen (Art. 42 Abs. 5 DS-GVO).

Zu Beginn des Jahres 2020 wurde eine Kooperationsvereinbarung zwischen den einzelnen Datenschutzaufsichtsbehörden und der DAkkS geschlossen, die die Details ihrer Zusammenarbeit im Rahmen des Akkreditierungsverfahrens regelt. Der Vertrag enthält beispielsweise Regelungen zur gegenseitigen Unterstützung der Aufsichtsbehörden untereinander, etwa um Fachpersonal bereitzustellen oder Mitarbeiter auszutauschen, aber auch zu Abläufen oder zur Gebührenverteilung.

In der Norm DIN EN ISO/IEC 17067:2013-12 „Konformitätsbewertung – Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme (ISO/IEC 17067:2013); Deutsche und Englische Fassung EN ISO/IEC 17067:2013“ wird die Festlegung von Prüfkriterien, -systematik und -methoden vorgegeben. Die abzuprüfenden datenschutzrechtlichen Anforderungen sind daher in einem Prüfkriterienkatalog vorzulegen (Art. 42 DS-GVO). Dieser ist in Form von Zertifizierungskriterien im Zertifizierungsprogramm der Zertifizierungsstelle oder des Programmeigners enthalten.

Im Berichtszeitraum wurde – in einem eigens eingerichteten UAK „Prüfkriterien“ – intensiv an einem Dokument zur einheitlichen Bewertung solcher Prüfkriterienkataloge gearbeitet.[16] Es beschreibt die Mindestanforderungen an die Zertifizierungskriterien, die ergänzend zu den Vorgaben der DIN EN ISO/IEC 17067 (Programmtyp 6) in einem

[16] Anforderungen an datenschutzrechtliche Zertifizierungsprogramme; Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Fertigstellung erst 2021.

Zertifizierungsprogramm enthalten sein müssen. Hinzu kommen ggf. noch Spezialanforderungen, die Berücksichtigung der EDSA-Leitlinien, etwa der „Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679“,[17] und z. B. von DSK-Beschlüssen.

Ziel war es, bestehende Anforderungen systematisch zu erfassen und unter Einbeziehung des SDM (s. Nr. 6.5) strukturiert aufzulisten, sodass eine potenzielle Zertifizierungsstelle, ein Programmeigner oder aber auch eine Datenschutzaufsichtsbehörde damit feststellen kann, ob ein Zertifizierungsprogramm vollständig, ausreichend dokumentiert und weitgehend mängelfrei ist. Für Zertifizierungsstellen soll es eine Erleichterung sein, damit diese wissen, was unbedingt in welcher Form enthalten sein muss. Aufsichtsbehörden sollen untereinander zu ähnlichen Bewertungen während einer Prüfung kommen, da die Arbeit aller Aufsichtsbehörden deutschlandweit Geltung bekommt und anhand der von einer Aufsichtsbehörde genehmigten Prüfkriterien akkreditierte Zertifizierungsstellen deutschlandweit anerkannt werden sollen.

Bislang gibt es in Sachsen-Anhalt noch keine nach Art. 42 und 43 DS-GVO akkreditierte Zertifizierungsstelle.

6.7 Windows 10

In seinem XVI. Tätigkeitsbericht (Nr. 6.8) stellte der Landesbeauftragte das von der DSK entwickelte Prüfschema „Datenschutz bei Windows 10“ vor. Das Prüfschema dient der juristischen Klärung, ob eine Telemetriedatenübermittlung an Microsoft rechtmäßig ist und auf welcher Rechtsgrundlage sie stattfinden kann. Verantwortliche mussten jedoch bei der Anwendung des Prüfschemas in den meisten Fällen die Rechtswidrigkeit der Telemetriedatenübermittlung feststellen, weil keine Erforderlichkeit dazu besteht und sich keine geeignete Rechtsgrundlage für die Telemetriedatenübermittlung an Microsoft finden lässt. Außerdem dürfte spätestens durch das „Schrems II“-Urteil (s. Nr. 5.2) eine Telemetriedatenübermittlung in die USA rechtswidrig sein. Es stand vielerorts die Frage im Raum, wie sich ein Verantwortlicher bei einer rechtswidrigen Telemetriedatenübermittlung an Microsoft durch das eingesetzte Betriebssystem Windows 10 zu verhalten hat.

Daher fasste die DSK am 26. November 2020 den Beschluss „Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise“.[18] Der Beschluss beruhte auf der Erkenntnis, dass Microsoft für die Enterprise-Edition des Betriebssystems für die Abschaltung der Telemetriefunktion, zumindest was personenbezogene Daten betrifft, eine Gruppenrichtlinie bereitgestellt hat, die von Administratoren zentral aktiviert werden kann. Diese Erkenntnis entstammt einer umfangreichen gemeinsamen technischen Prüfung der Niedersächsischen Landesbeauftragten für den Datenschutz und des Bayerischen Landesamts für Datenschutzaufsicht unter Konsultation Microsofts.[19] Das BSI ist in einer anderen Prüfung zu dem Ergebnis gekommen, dass trotz der o. g. Gruppenrichtlinie weiterhin Daten an Microsoft fließen können und dass Microsoft über

[17] https://lsaurl.de/EDSALeitlinien12018

[18] https://lsaurl.de/DSKWin10

[19] https://lsaurl.de/DSKWin10Anlage1

bestimmte Serveradressen die Einstellungen der Gruppenrichtlinie rückgängig machen könnte.[20]

Beide Untersuchungsergebnisse werden in dem Beschluss zusammenfassend dargestellt. Anschließend werden darin folgende Konsequenzen für Verantwortliche erörtert: Verantwortliche müssen gemäß o. g. Prüfschema die Rechtmäßigkeit der Telemetriedatenübermittlung nachweisen oder diese unterbinden. Zum Unterbinden der Datenübermittlung kann die o. g. Gruppenrichtlinie namens „Telemetrielevel Sicherheit“ zumindest in der Enterprise-Edition genutzt werden, jedoch muss gleichzeitig durch zusätzliche Maßnahmen wie Internetfilter die Verhinderung der Telemetriedatenübermittlung sichergestellt werden.

Abschließend stellt die DSK fest, dass aufgrund der fortlaufenden Weiterentwicklung des Betriebssystems die o. g. Untersuchungsergebnisse die Verantwortlichen nicht endgültig von ihrer aus Art. 5 Abs. 2 DS-GVO resultierenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten können. Dies gilt umso mehr für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen.

In der Geschäftsstelle des Landesbeauftragten wurde das Betriebssystem Windows 7 nach dem Supportende im Jahre 2020 durch Windows 10 Enterprise abgelöst. Auch der Landesbeauftragte achtet darauf, dass neben der oben genannten Gruppenrichtlinie „Telemetrielevel Sicherheit“ weitere Maßnahmen, wie Deaktivierung des Betriebssysteminternen Diagnosedienstes, Sperren bestimmter Domainadressen von Microsoft und Isolierung des internen Netzwerks vom Internet, umgesetzt sind.

6.8 Microsoft Office 365

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

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

Beim Einsatz von MS 365 handelt der Nutzer als Verantwortlicher (Art. 4 Nr. 7 DS-GVO) und Microsoft regelmäßig als Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO). Die

[20] https://lsaurl.de/DSKWin10Anlage2

DS-GVO benennt die zu prüfenden Kriterien, die ein Auftraggeber als Verantwortlicher zu berücksichtigen hat:

Einem Verantwortlichen obliegt es zunächst gem. Art. 32 Abs. 1 DS-GVO, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Kategorien personenbezogener Daten festzustellen und basierend darauf die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener natürlicher Personen zu beurteilen. Je nachdem, ob nur pseudonyme Metadaten in einer Ende-zu-Ende-verschlüsselten Videokonferenz oder detaillierte Bürger- oder Schülerdaten in einer Cloud verarbeitet werden, wird das Ergebnis stark variieren.

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

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

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

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

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

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

- Bei der Auftragsverarbeitung stellt Art. 28 DS-GVO genaue Anforderungen an die Inhalte des zugehörigen Vertrages. In den Dokumenten von MS 365 finden

sich jedoch unpräzise Beschreibungen zu Arten und Zwecken der Datenverarbeitungen und den betroffenen personenbezogenen Daten.

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

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

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

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

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

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

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

Der Landesbeauftragte wurde durch eine Behörde gefragt, ob es datenschutzrechtlich möglich sei, eine deutlich kostengünstigere MS 365-Lizenzierung lediglich zum Zweck der Lizenzüberprüfung (und Vertragsverlängerung) einer bestehenden On-Premises-

[21] Microsoft Online Services Subprocessor List, https://go.microsoft.com/fwlink/p/?linkid=2096306

[22] https://lsaurl.de/EDSA012020

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

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

In dem durch die Behörde angestrebten aktuellen Pilotprojekt mit:

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

sind die vorgenannten Kritikpunkte an MS 365 weniger schwerwiegend.

Bezüglich der im Raum stehenden Absicht des Abschlusses eines Landesvertrages zur Auftragsverarbeitung wurde vorsorglich auf die Einhaltung des Landesrechts (§ 15 Abs. 2 DSAG LSA – Unterwerfungspflicht des Auftragsverarbeiters) hingewiesen. Im

[23] https://docs.microsoft.com/de-de/lifecycle/products/?products=office

Raum steht aber auch die Nutzung eines möglicherweise zukünftigen Bundes-Rahmenvertrages in einer Bundes-Cloud oder auch die Nutzung des Phoenix-Arbeitsplatzes von Dataport. Eine Entscheidung ist hier durch das Ministerium der Finanzen zu fällen.

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

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

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

6.9 Mobiles Arbeiten – Home-Office

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

Die vorgenannten Themenbereiche fließen unterschiedlich stark in den Komplex Home-Office ein. So sollte Telearbeit, sofern Fernzugriffe auf unternehmens- bzw. behördeninterne Strukturen erfolgen, durch VPN-Kanäle abgesichert sein oder über sichere webbasierte Kollaborationsplattformen erfolgen. Der Einsatz privater Geräte bei der Verarbeitung betrieblicher bzw. dienstlicher Daten sollte generell vermieden oder nur unter strengen Vorgaben im Rahmen eines gut organisierten Mobile Device Managements durchgeführt werden. Mobile Datenträger und Geräte wie Laptops, Tablets und Smartphones sollten generell verschlüsselt sein. Der Zugang zu diesen Geräten sollte, wenn möglich, nur mit Zwei-Faktor-Authentifizierung oder zumindest mit sicheren Passwörtern ermöglicht werden. Bei der Nutzung von Chat- und Videokonferenzdiensten sollten geeignete Dienstleister ausgewählt und vertragliche Rahmenbedingungen berücksichtigt werden. Dies gilt auch für den Einsatz von Kollaborationsplatt-

formen. Generell sollten personenbezogene Daten so wenig wie möglich die Unternehmens- bzw. Behördenstrukturen verlassen und wenn, dann nur verschlüsselt. Des Weiteren sollte zunächst immer erst der Eigenbetrieb vorgenannter Dienste in Betracht gezogen werden. Beim Einsatz von Dienstleistern ist von Anbietern aus unsicheren Drittländern Abstand zu nehmen und sind die Vorgaben des Art. 28 DS-GVO zu beachten. Außerdem sollten Verschlüsselungsmechanismen immer nach dem Stand der Technik implementiert sein und zusammen mit sicheren Passwörtern zur Anwendung kommen.

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

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

Der CIO des Landes Sachsen-Anhalt erstellt derzeit eine Informationssicherheitsrichtlinie zum Thema Telearbeit. Anlass dafür war der Beschluss des Landtages (LT-Drs. 7/2933) vom 24. Mai 2018 mit dem die Landesregierung aufgefordert wurde, ein Konzept zur Förderung und Umsetzung von Telearbeit für die unmittelbare Landesverwaltung zu erarbeiten. Dazu sollte eine umfassende Bestandsaufnahme zur Telearbeit vorgelegt werden, was mit dem Bericht „Telearbeit in der Landesverwaltung Sachsen-

[24] https://lsaurl.de/BSIMobilArbeiten

[25] https://lsaurl.de/BSIHomeOffice

Anhalt“ inklusive eines Entwurfs einer Rahmenrichtlinie über flexibles Arbeiten in Telearbeit in der Landesverwaltung des Landes Sachsen-Anhalt (LT-Drs. 7/5474) erfolgte. Diese Unterlagen dienten als Grundlage für die weitere Behandlung in den zuständigen Ausschüssen für Inneres und Sport, für Finanzen, für Wirtschaft, Wissenschaft und Digitalisierung sowie für Arbeit, Soziales und Integration.

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

6.10 Sicherer E-Mailversand

Im Frühjahr 2020 wurde die vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ vorgelegte Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“[26] durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder mit Mehrheitsbeschluss verabschiedet und in der Folge aktualisiert.

Der unverschlüsselte Versand personenbezogener Daten per E-Mail war lange Zeit viel zu wenig hinterfragte Praxis. Warnungen der Datenschützer wurden oft mangels Verschlüsselungs-Know-how in Verbote umgemünzt, da keine durchgängige Sicherheit gewährleistet werden konnte. Der Warner wurde so ungewollt zum Verhinderer. Zur effizienten Kommunikation wurden Alternativen gesucht und nicht zuletzt häufig in sozialen Netzwerken und Messengern gefunden. E-Mail ist aber trotz oder gerade aufgrund der immanenten technologischen Rückständigkeit ein einfach zu nutzendes, weit verbreitetes und mittelfristig nicht wegzudenkendes Medium. Die DSK versuchte daher bereits seit jeher, den Status Quo zu verbessern. Das Thema E-Mail hat mit verschiedenen Schwerpunkten auch eine dauerhafte Position im Tätigkeitsbericht des Landesbeauftragten.

Während im XIII./XIV. Tätigkeitsbericht (Nrn. 4.10, 4.11) noch die Einführung von TLS-basierter Verschlüsselung nach dem Stand der Technik nahegelegt wurde, hat sich die Situation mittlerweile verbessert. Das Land Sachsen-Anhalt führte 2018 TLS 1.2 für den Landes-E-Mail-Server ein und immer mehr E-Mail-Provider rüsteten ebenso auf. Eine durchgehende Transportverschlüsselung ist mittlerweile nicht nur Stand der Technik, sondern auch unter Beachtung der in Art. 32 Abs. 1 DS-GVO zu berücksichtigenden Aspekte obligatorisch umzusetzen. Der nächste Schritt sollte es damals sein, die Annahme unverschlüsselter E-Mails zu verweigern (nur noch SSL/TLS, kein STARTTLS oder gar unverschlüsseltes SMTP mehr). Grund ist, dass bei der Nutzung von STARTTLS der erste Verbindungsaufbau immer im Klartext erfolgt und für Man-in-the-Middle-Angriffe (Downgrade-Angriffe durch Verhinderung der TLS-Verschlüsselung) anfällig ist, sofern keine Gegenmaßnahmen getroffen wurden

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

(DANE, MTA-STS). Da STARTTLS keine Vorteile gegenüber TLS bietet, wird die Einstellung von „SSL/TLS“ in E-Mail-Clients empfohlen und von der Nutzung von STARTTLS (insbesondere auf den Landes-E-Mail-Servern) abgeraten. Es wird dem Land empfohlen, zumindest innerhalb des Landesnetzes den unverschlüsselten Empfang und Versand komplett zu unterbinden.

Doch welche technischen und organisatorischen Maßnahmen müssen konkret getroffen werden, um ein angemessenes Schutzniveau zu erreichen? Wie sind Geschäftsgeheimnisse und personenbezogene Daten in E-Mails sicher übermittelbar? Genügt eine Transportverschlüsselung? Ab wann wird eine zusätzliche Verschlüsselung benötigt, wann eine Ende-zu-Ende-Verschlüsselung? Was ist bei der Umsetzung der verschiedenen Möglichkeiten in der Praxis zu beachten? Wo gibt es weitere Hinweise? Die eingangs genannte Orientierungshilfe versucht, solche Fragen zu beantworten und gibt konkrete Handlungsempfehlungen.

Verantwortliche müssen die Risiken, die durch die Übermittlung personenbezogener Daten per E-Mail entstehen, mit geeigneten technischen und organisatorischen Maßnahmen mindern (Art. 25 DS-GVO). Dabei sind der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung, sowie Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. In der Orientierungshilfe erläutert die Datenschutzkonferenz, was genau alles beim Versand und Empfang von E-Mail-Nachrichten zu beachten ist und welche Anforderungen Verfahren zur Verschlüsselung erfüllen müssen, um der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen.

Sowohl Transportverschlüsselung als auch Ende-zu-Ende-Verschlüsselung mindern die bestehenden Risiken für die Vertraulichkeit und Integrität der übertragenen personenbezogenen Daten. Beide Verfahren müssen durch Verantwortliche bei der Wahl der technischen und organisatorischen Maßnahmen berücksichtigt und möglichst kombiniert werden.

Für Ende-zu-Ende-Verschlüsselungen werden in der Orientierungshilfe S/MIME und OpenPGP in den jeweils aktuellen Standards abschließend aufgezählt.

Der Landesbeauftragte bittet an dieser Stelle, insbesondere das „sichere“ Verfahren Chiasmus des BSI nur mit Vorsicht und Bedacht einzusetzen. Zum einen werden Passwörter/Schlüssel durch Verantwortliche im Land auch per E-Mail verschickt (bitte nicht nachmachen). Zum anderen enthält das Programm eine „selbstentwickelte“, weitgehend proprietäre Kryptografie, welche verglichen mit den etablierten Standards wenig zum Einsatz kommt und damit auch weniger in der Praxis untersucht wurde.

Die Nutzung der Transportverschlüsselung bietet lediglich einen Basis-Schutz und stellt damit auch nur eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Abhängigkeit von den mit der Übertragung per E-Mail verbundenen Risiken kann eine Transportverschlüsselung im Normalfall bereits ausreichend sein. Zur Sicherstellung einer durchgehenden qualifizierten Transportverschlüsselung müssen Serverbetreiber und Nutzer aktiv werden.

Der Landesbeauftragte legt allen Verantwortlichen, den von diesen eingebundenen Auftragsverarbeitern und genutzten öffentlichen E-Mail-Diensteanbietern nahe, die in der Orientierungshilfe der DSK genannten Anforderungen umzusetzen.

6.11 ITN-XT – Sachstand

In seinem XV. Tätigkeitsbericht (Nr. 5.1) berichtete der Landesbeauftragte über die damals für die Anbindung aller Behördenstandorte in Sachsen-Anhalt an das ITN-XT erforderlichen Standortbegehungen unter enger Einbeziehung des Landesbetriebs Bau- und Liegenschaftsmanagement Sachsen-Anhalt (BLSA). Anschließend wurden im Jahr 2019 und 2020 zahlreiche Standorte während der sog. WAN-Migration BSI-Grundschutz-konform an das Backbone-verschlüsselte ITN-XT mittels entsprechender Kryptokomponenten angebunden, so auch die Geschäftsstelle des Landesbeauftragten.

Bemerkenswert ist, dass Standorte im Vorfeld der Migration genau anzugeben haben, auf welchen Netzwerkrouten welche Ziele erreicht werden können müssen. Lediglich die geplanten Routen werden nach der Migration auch tatsächlich geschaltet. Somit wird verhindert, dass ein WAN-Anschluss einer Behörde beliebig ins ITN-XT kommunizieren kann. Standorte können dann nur mit den vorher festgelegten Gegenstellen und den Fachverfahren in den Rechenzentren von Dataport kommunizieren.

Für die Behördenarbeit erforderliche Kommunikationswege und Kommunikationsprotokolle, die über einen gewissen vordefinierten Landesstandard hinausgehen, müssen schriftlich dokumentiert und als sog. „Change-Requests“ über einen formellen Weg beantragt werden. Dabei kommt dem Betriebszentrum des ITN-XT im Ministerium der Finanzen eine zentrale koordinierende Rolle zu, denn dieses gibt über das Extranet des Landes die zahlreichen Formulare für etwaige Änderungsanträge vor, nimmt jegliche Meldungen zum ITN-XT entgegen und leitet diese nach formaler und inhaltlicher Prüfung dem Dienstleister T-Systems zu, der für die praktische Realisierung etwaiger Anträge zuständig ist.

So müssen z. B. Schranköffnungen an den Gebäudeverteilern, in denen die Hardware der WAN-Übergänge verbaut ist, schriftlich im Betriebszentrum angemeldet werden, damit diese bei T-Systems für den beantragten Zeitraum aus der Überwachung genommen werden. Würde dies nicht gemeldet werden, so würde bei einer unautorisierten Schranköffnung ein elektronischer Alarm bei T-Systems auflaufen. Je nach Standort, Tageszeit und Erreichbarkeit eines Standortverantwortlichen kann dies sogar dazu führen, dass der Alarmzustand bis an die örtliche Polizeibehörde eskaliert und ein Streifenwagen an den Standort entsendet wird, um vor Ort die Sicherheitslage zu überprüfen.

Die vorgenannten technischen und organisatorischen Maßnahmen bei der Umsetzung des ITN-XT sind dem Ziel geschuldet, ein nach BSI-Grundschutz zertifiziertes sicheres Landesnetz aufzubauen. Durch diese Bestrebungen wird tatsächlich ein höheres Sicherheitsniveau bei der Datenübermittlung zwischen Behörden der Landesverwaltung sowohl untereinander als auch zu deren Dienstleistern erreicht. Dies ermöglicht es der Landesverwaltung auch in Zukunft personenbezogene Daten, deren Missbrauch mit erhöhten Risiken für die Rechte und Freiheiten der Betroffenen verbunden wäre, datenschutzkonform über Standortgrenzen hinweg zu übermitteln.

Während die erste Ausbaustufe (WAN-Migration aller Standorte) zum Jahreswechsel 2020/21 noch nicht ganz abgeschlossen war, hat das Betriebszentrum an ausgewählten Standorten bereits mit der nächsten Ausbaustufe begonnen. Dabei werden ausgehend von den grundschutzkonformen Gebäudeverteilern die Etagenverteiler mit entsprechenden Switches, die wie die WAN-Komponenten durch T-Systems als Dienstleister betreut werden, ausgestattet, so dass das ITN-XT bis in die Büros hinein umgesetzt ist. Dies ist Voraussetzung dafür, dass in einer weiteren Ausbaustufe die IP-basierte Telefonie aus Los 2 der ITN-XT-Ausschreibung in den Standorten umgesetzt werden kann. Der Landesbeauftragte begrüßt die vorgenannten Bestrebungen des CIO ausdrücklich und wird den Fortgang des Projektes weiterhin verfolgen.

6.12 Videokonferenzsysteme

Mit Beginn der Corona-Pandemie wurden vielerorts Ausgangsbeschränkungen festgelegt, Dienstreisen und Gremiensitzungen vermieden und Teile des Arbeitslebens sowie schulische und Fortbildungs-Tätigkeiten in den privaten Wohnraum verlagert. Einhergehend mit diesen Anpassungen an die gesellschaftliche Situation ist der Einsatz von Videokonferenzlösungen in kürzester Zeit das Mittel der Wahl geworden, um Distanzen zu überbrücken und geschäftliche, dienstliche und schulische sowie fortbildende Tätigkeiten fortführen zu können.

Das Durchführen einer Videokonferenz ist eine Verarbeitung personenbezogener Daten, denn es werden von allen Teilnehmern mindestens zeitweise Bild- und Tondaten an ein zentrales System übertragen und von dort den jeweils anderen Teilnehmern weitergeleitet. Somit ist der Veranstalter einer Videokonferenz Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO und hat zahlreiche rechtliche Vorgaben der Datenschutz-Grundverordnung zu erfüllen. Wird zur Durchführung einer Videokonferenz die Plattform eines Dienstleisters in Anspruch genommen, so handelt es sich um eine Auftragsverarbeitung gem. Art. 28 DS-GVO, die entsprechend vertraglich unterlegt sein muss.

Die DSK hat dies zum Anlass genommen, eine Orientierungshilfe[27] zum Thema Videokonferenzsysteme zu erarbeiten, welche am 23. Oktober 2020 veröffentlicht wurde.

Die Orientierungshilfe unterscheidet zunächst die drei Betriebsmodelle Eigenbetrieb, Betrieb durch Dienstleister und Nutzung eines Online-Dienstes. Des Weiteren werden die rechtlichen Anforderungen für die jeweiligen Betriebsmodelle dargestellt. Hier werden auch mögliche Rechtsgrundlagen für die Verantwortlichen und die damit einhergehende Zweckbindung erörtert. So wird zum Beispiel auf die Einwilligung als mögliche Rechtsgrundlage eingegangen oder die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO näher beleuchtet. Anschließend werden die Pflichten des Verantwortlichen aufgelistet. Hierbei sind vor allem die Informationspflichten an die Betroffenen, die rechtmäßige Ausgestaltung einer Auftragsverarbeitung und die rechtssichere Datenübermittlung in Drittländer von Bedeutung. Abschließend werden technische und organisatorische Anforderungen an die Durchführung einer Videokonferenz dargestellt. Dabei wird auf Themen wie Übertragungssicherheit,

[27] https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf

Nutzerauthentifizierung, Softwareaktualisierung, Rollentrennung oder Konferenzaufzeichnung eingegangen.

Vor dem Hintergrund des „Schrems II“-Urteils (s. Nr. 5.2) wird von den Aufsichtsbehörden die Nutzung von Online-Diensten US-amerikanischer Anbieter besonders kritisch gesehen. Die Anbieter beziehen sich dann zwar auf ihre Standardvertragsklauseln, die allerdings ohne zusätzliche Sicherungsmaßnahmen nicht ausreichend sein dürften. Besonders problematisch ist es, wenn derlei Produkte in Schulen eingesetzt werden, da bei der Verarbeitung personenbezogener Daten von Kindern und Jugendlichen gem. ErwGr 38 DS-GVO besonders hohe Anforderungen gelten.

Die Datenschutzaufsichtsbehörden verschafften sich einen Überblick über Anbieter und deren Produkte zur Durchführung von Videokonferenzen und haben diese im Einzelfall geprüft. Schließlich nahmen sie auch selbst an Videokonferenzen teil, oft auch als Veranstalter. Der Landesbeauftragte gibt allerdings weder Produkte frei, noch spricht er sich generell gegen deren allgemeine Verwendung aus. Jeder Einsatz einer Videokonferenzlösung ist als Einzelfall zu betrachten und in seiner rechtlichen Würdigung abhängig davon, ob und welche personenbezogenen Daten, welcher Betroffenenkreise, zu welchen Zwecken, in welchem Umfang in einer Videokonferenz verarbeitet werden und wie die vertragliche Ausgestaltung umgesetzt ist. Schließlich sind die öffentlichen und nichtöffentlichen Stellen selbst in der Verantwortung, eine rechtskonforme Lösung für das gestellte Ziel zu erarbeiten und umzusetzen und im Zweifelsfall auch Verantwortung für Fehlentscheidungen zu tragen. Der Landesbeauftragte behält es sich als Aufsichtsbehörde vor, jederzeit den Einsatz von Videokonferenzsystemen im öffentlichen und nichtöffentlichen Bereich zu kontrollieren und ggf. auch zu untersagen oder zu sanktionieren, wenn erforderlich.

Auch das BSI erstellte ein Papier zu diesem Thema. Am 16. März 2021 legte das BSI in einem neuen Mindeststandard für Videokonferenzen[28] Sicherheitsanforderungen vor, die sich auf den Erhalt der Vertraulichkeit in digitalen Konferenzen fokussieren.

6.13 Informationssicherheit

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

[28] https://lsaurl.de/BSIVideokonferenz

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

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

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

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

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

7 Telekommunikation und Medien

7.1 Webtracking – Google Analytics

In seinem XVI. Tätigkeitsbericht (Nr. 7.1) hatte der Landesbeauftragte bereits auf die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlichte Orientierungshilfe für Anbieter von Telemedien sowie

die in einer abgestimmten Aktion der Datenschutzaufsichtsbehörden herausgegebenen Mitteilungen zum Einsatz von Google Analytics und ähnlichen Analysediensten hingewiesen.

Allerdings bestand hinsichtlich des Einsatzes von Google Analytics weiterhin großer Beratungsbedarf, da es sich um das meistgenutzte Analysetool handelt, mit dessen Hilfe sich umfassende statistische Auswertungen des Nutzungsverhaltens der Webseitenbesucher vornehmen lassen.

Aus diesem Grund haben die Datenschutzaufsichtsbehörden den Einsatz von Google Analytics noch einmal neu bewertet. Die Ergebnisse wurden in dem Beschluss „Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich“ der DSK vom 12. Mai 2020 veröffentlicht.[29]

Demnach sind Google und der Google-Analytics-Anwender unter Berücksichtigung der aktuellen Rechtsprechung des Europäischen Gerichtshofs[30] gemeinsam für die Datenverarbeitung verantwortlich. Unter Anwendung dieser Grundsätze geht der Landesbeauftragte derzeit davon aus, dass im Fall der Weiterverarbeitung durch Google zu eigenen Zwecken eine gemeinsame Verantwortung gem. Art. 26 DS-GVO besteht. Dies ist aber auf der europäischen Ebene noch nicht abschließend geklärt.

Sollten Webseitenbetreiber nicht auf alternative und datensparsame Werkzeuge zur Reichweitenmessung ausweichen, sondern weiterhin Google Analytics verwenden, werden Maßnahmen in dem DSK-Beschluss aufgelistet, die dafür zwingend umzusetzen sind. Die darin getroffene Feststellung, dass ein rechtmäßiger Einsatz von Google Analytics in der Regel nur aufgrund einer wirksamen Einwilligung der Webseitenbesucher gem. Art. 6 Abs. 1 lit. a i. V. m. Art. 7 DS-GVO möglich ist, wurde durch das Urteil des Bundesgerichtshofs vom 28. Mai 2020 (I ZR 7/16 – „Planet49“) bestätigt.

7.2 TTDSG – Umsetzung der E-Privacy-Richtlinie

In seinem XVI. Tätigkeitsbericht (Nr. 7.1) hatte der Landesbeauftragte bereits auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 1. Oktober 2019 hingewiesen (Az. C-673/17, „Planet49“). Dieser hatte entschieden, dass eine wirksame Einwilligung nach den Vorgaben der E-Privacy-Richtlinie 2002/58/EU aktiv erteilt werden muss. Demnach kann die für die Speicherung und den Abruf von Cookies auf dem Gerät des Besuchers einer Webseite erforderliche Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht wirksam erteilt werden.

Der Bundesgerichtshof (BGH) ist in seinem Urteil vom 28. Mai 2020 (Az. I ZR 7/16) der Vorabentscheidung des EuGH gefolgt und hat das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies bestätigt. Dabei geht der BGH davon aus, dass sich § 15 Abs. 3 Satz 1 Telemediengesetz (TMG) europarechtskonform auslegen lässt. Entsprechend dem Wortlaut wäre die Datenverarbeitung zulässig, wenn der Betroffene entsprechend informiert wurde und nicht widersprochen hat (sog.

---

[29] https://lsaurl.de/DSKGoogleAnalytics

[30] Urteil vom 1. Oktober 2019, Az. C-673/17 („Planet49“) und Urteil vom 29. Juli 2019, Az. C-40/17 („Fashion ID“)

Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 E-Privacy-Richtlinie legt der BGH § 15 Abs. 3 TMG jedoch dahingehend aus, dass schon in dem Fehlen einer wirksamen Einwilligung ein solcher Widerspruch gesehen werden kann und deshalb eine aktive Einwilligung erforderlich ist.

Kurz nach dem BGH-Urteil wurde der Entwurf für ein Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze (Telekommunikation-Telemedien-Datenschutzgesetz – TTDSG) veröffentlicht.[31] Der Gesetzentwurf enthielt Datenschutzbestimmungen, die bisher im Telekommunikationsgesetz und im TMG enthalten waren und führte so den Telekommunikationsdatenschutz und den Telemediendatenschutz in einem neuen Gesetz zusammen. Dabei wurden auch notwendige Anpassungen an die europäischen Vorgaben der DS-GVO und der E-Privacy-Richtlinie vorgenommen.

Da der Entwurf des TTDSG jedoch hinter einer europarechtskonformen Umsetzung der E-Privacy-Richtlinie sowie den Anforderungen einer Anpassung an die DS-GVO zurückblieb, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im November 2020 eine Entschließung veröffentlicht, die den Bundesgesetzgeber auffordert, die europarechtlichen Verpflichtungen der E-Privacy-Richtlinie endlich zu erfüllen und in nationales Recht umzusetzen **(Anlage 8)**.

7.3 Verantwortlichkeit für Facebook-Fanpages

Wie bereits in seinen früheren Tätigkeitsberichten hat der Landesbeauftragte auch im XVI. Tätigkeitsbericht (Nr. 7.2) den öffentlichen und nichtöffentlichen Stellen vom Betrieb einer Facebook-Fanpage abgeraten.

Als Folge einer solchen Beratung hatte die Staatskanzlei die Facebook-Fanpage des Landes wegen durchgreifender rechtlicher Bedenken und haftungsrechtlicher Risiken zunächst abgeschaltet, reaktivierte sie jedoch im Zuge der Corona-Pandemie im März 2020. Die Wiederaufnahme des Betriebs der Facebook-Fanpage sah der Landesbeauftragte kritisch, auch wenn über diesen Kanal nur Informationen zur Corona-Pandemie veröffentlicht wurden.

7.4 Der neue Medienstaatsvertrag

Bereits Ende 2019 haben die Länder einen neuen Medienstaatsvertrag (MStV) beschlossen, der am 7. November 2020 in Kraft getreten ist. Der MStV löst den seit 1991 geltenden Rundfunkstaatsvertrag ab und erfasst nicht mehr nur Radio- und Fernsehsender, sondern zusätzlich auch solche Anbieter, die Medieninhalte vermitteln bzw. deren Verbreitung dienen – sog. Gatekeeper (z. B. Suchmaschinen, Streaming-Anbieter, Sprachassistenten, App-Stores, soziale Netzwerke). Er enthält grundlegende Regelungen für die Veranstaltung und das Angebot, die Verbreitung und die Zugänglichmachung von Rundfunk und Telemedien in Deutschland.

Mit dem MStV werden die Vorgaben aus der „EU-Richtlinie für audiovisuelle Mediendienste“ in nationales Recht umgesetzt. Diese Regelungen, sowohl auf EU- als auch

[31] Das Gesetz wurde nach dem Ende des Berichtszeitraums zwischenzeitlich mit Wirkung zum 1. Dezember 2021 in Kraft gesetzt.

auf nationaler Ebene, stärken den Jugendmedienschutz, gewährleisten mehr Transparenz im Hinblick auf den Meinungsbildungsprozess und sichern den Medienpluralismus und somit die Meinungsvielfalt. Zentraler Punkt ist die diskriminierungsfreie Auffindbarkeit und Präsentation von Angeboten oder Inhalten, das heißt, dass Algorithmen bestimmte Onlineangebote nicht gezielt bevorzugen oder benachteiligen dürfen.

Wie im bisherigen Rundfunkstaatsvertrag gilt auch im MStV für die Datenverarbeitung zu journalistisch-redaktionellen Zwecken das sog. Medienprivileg (vgl. §§ 12, 23 MStV). Für Sachsen-Anhalt folgt damit aus § 12 Abs. 4 MStV i. V. m. § 38 Abs.1 MDR-Staatsvertrag der aktuellen Fassung, dass die datenschutzrechtliche Zuständigkeit des Landesbeauftragten für den öffentlich-rechtlichen Rundfunk – also den Mitteldeutschen Rundfunk (MDR) – nicht gegeben ist.

Ebenso ist die datenschutzrechtliche Zuständigkeit des Landesbeauftragten nicht gegeben, soweit Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen. In diesen Fällen ist der Deutsche Presserat anstelle des Landesbeauftragten für die Beachtung der datenschutzrechtlichen Vorschriften zuständig. Er prüft Beschwerden in einem eigenen Redaktionsdatenschutz-Ausschuss.

Dies gilt allerdings nur für den journalistisch-redaktionellen Bereich. Für alle sonstigen Bereiche der Presseunternehmen wie Verwaltung, Abonnements, Nutzungsdaten der Webseite etc. gilt die DS-GVO uneingeschränkt und ist der Landesbeauftragte für die Aufsicht über deren Einhaltung zuständig.

8 Öffentliche Sicherheit

8.1 Polizei 2020

Mit dem von der Innenministerkonferenz beschlossenen Programm „Polizei 2020“ wollen die Polizeien von Bund und Ländern die polizeiliche Informationsarchitektur zukunftsfähig gestalten. Bisher verfügen die Polizeien der Länder über keine einheitliche Informationsarchitektur, die einen schnellen Austausch von Daten zulässt. Das Programm „Polizei 2020“ soll die verschiedenen Datenbestände verknüpfen und die vorhandenen Informationen für alle Polizistinnen und Polizisten im Rahmen der ihnen zugewiesenen Aufgaben nutzbar machen.

Im Jahr 2020 legten die Polizeien von Bund und Ländern einen ersten „fachlichen Bebauungsplan“ für das Programm „Polizei 2020“ vor. Dieser benennt den Datenschutz als eines der Kernziele des Programms. Diese Zielstellung wurde von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ausdrücklich begrüßt. Gleichwohl wurde das Fehlen von konkreten Vorschlägen zur Stärkung des Datenschutzes bei der Umsetzung des Projektes kritisiert. Die DSK hat deshalb mit ihrer Entschließung „Polizei 2020 – Risiken sehen, Chancen nutzen!“ vom 16. April 2020 **(Anlage 2)** datenschutzrechtliche Kernforderungen formuliert, deren Berücksichtigung sie bei der Umsetzung des Programms „Polizei 2020“ als zwingend erachtet.

Der Landesbeauftragte wird die Entwicklung des Programms „Polizei 2020“ in enger Abstimmung mit dem Bundesbeauftragten und den Landesbeauftragten der anderen Bundesländer weiterhin kritisch begleiten.

8.2 Länderübergreifendes Glücksspielauswertesystem

Der Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (Staatsvertrag) vom 29. Oktober 2020 dient insbesondere der bundesweiten Legalisierung und Regulierung des Online-Glücksspiels. Zur Wahrnehmung der Glücksspielaufsicht beschlossen die Länder, zum 1. Juli 2021 eine rechtsfähige Anstalt des öffentlichen Rechts als „Gemeinsame Glücksspielbehörde der Länder“ (Aufsichtsbehörde) mit Sitz in Sachsen-Anhalt zu errichten.

Aufgaben dieser Aufsichtsbehörde sind u. a. die Ausübung der Aufsicht über Veranstalter von Sportwetten im Internet, Online-Poker und virtuellen Automatenspielen im Internet.

Das Länderübergreifende Glücksspielauswertesystem (LUGAS) dient der Aufsichtsbehörde als Instrument zur bundesweit einheitlichen Überwachung des Online-Glücksspiels und der Glücksspielanbieter. Zur effektiven Überwachung ist es erforderlich, personenbezogene Daten des Spielers (u. a. Name, Anschrift, Geburtsdatum, Geburtsort, Höhe des vom Spieler festgelegten anbieterübergreifenden Einzahlungslimits) zu verarbeiten und regelmäßig zu aktualisieren. Im Zuge dieser Verarbeitung wird die Glücksspiel-Aufsichtsbehörde zur Verantwortlichen i. S. der DS-GVO, über die der Landesbeauftragte die datenschutzrechtliche Aufsicht ausübt.

Glücksspielanbieter müssen vielfältige Bedingungen zum Schutz der Spieler einhalten, u. a. auch ein auf wissenschaftlichen Erkenntnissen beruhendes, automatisiertes System zur Spielsuchtfrüherkennung implementieren. Zu diesem Zweck sind Glücksspielanbieter verpflichtet, die für die Glücksspielaufsicht notwendigen Daten digital unveränderlich und jederzeit kontrollierbar zu erfassen. Dazu betreiben Glücksspielanbieter Server, auf welche die Aufsichtsbehörde zur Überwachung der Aktivitäten von Glücksspielanbietern über ein Auswertesystem zugreift.

Die Behörde führt zum Schutz der Spieler vor den Gefahren der Spielsucht drei Dateien: eine Aktivitätsdatei zur Verhinderung parallelen Spiels bei mehreren Glücksspielanbietern, eine Limitdatei zur anbieterübergreifenden Einzahlungslimitierung und eine Spielersperrdatei zur Selbst- oder Fremdsperre eines Spielers. Ihre rechtliche Grundlage finden die drei Dateien im Staatsvertrag.

Der Landesbeauftragte wurde durch das federführende Ministerium für Inneres und Sport des Landes Sachsen-Anhalt frühzeitig in die Projektgruppe zur Erarbeitung des LUGAS eingebunden. Über die Teilnahme an verschiedenen Projektgruppensitzungen und die Erarbeitung datenschutzrechtlicher Stellungnahmen durch den Landesbeauftragten flossen die Belange des Datenschutzes umfassend in die Projektarbeit ein. Insbesondere wurden Fragen zur Anonymisierung von Spielerdaten mit dem Ziel erörtert, den „gläsernen Spieler“ zu vermeiden.

Aufgrund der vertrauensvollen und konstruktiven Zusammenarbeit in der Projektgruppe konnte der Landesbeauftragte maßgeblich Einfluss auf die Ausgestaltung des

LUGAS nehmen und im Ergebnis gewährleisten, dass die Verarbeitung der personenbezogenen Daten auf das erforderliche Mindestmaß beschränkt wird.

8.3 Schutz vertraulicher Kommunikation – § 113 TKG

Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Bundesverfassungsgericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs- und Abrufregelungen müssen die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden. Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe korrespondierender fachgesetzlicher Abrufregelungen wurden für mit dem Grundgesetz unvereinbar erklärt.

Mit der Entschließung vom 25. November 2020 **(Anlage 9)** appellierte die DSK an die Gesetzgeber auf Bundes- und Landesebene, alle Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts zu evaluieren und gegebenenfalls anzupassen. Weiterhin hielt es die DSK für geboten, dass die politisch Verantwortlichen die vom Bundesverfassungsgericht gesetzte Frist nicht ausreizen und das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform ausgestalten.

9 Verkehr

9.1 Datenschutzrechtliche Verwertungsverbote im Führerscheinwesen

Die Beschwerde eines Führerscheininhabers, der von der Führerscheinstelle verpflichtet wurde, ein Fahreignungsgutachten bei einer Begutachtungsstelle in Auftrag zu geben, gab Anlass, die Datenübermittlung der Führerscheinstelle an den Gutachter zu überprüfen. In den Stellungnahmen im Rahmen der Anhörung durch den Landesbeauftragten bekräftigte die Fahrerlaubnisbehörde, dass sie immer die vollständigen Unterlagen an die MPU-Stelle (Gutachter, der die medizinisch-psychologische Untersuchung durchführt) übersende. Die Fahrerlaubnisbehörden seien nicht befugt, die Akten zu kürzen. Die Einschätzung, welche Unterlagen benötigt werden, treffe die MPU-Stelle.

Der Landesbeauftragte hat die Beschwerde mit dem Landesverwaltungsamt Halle als Aufsichtsbehörde unter Einbeziehung des zuständigen Landesministeriums ausgewertet und die Führerscheinstelle gewarnt, zukünftig nicht an der mitgeteilten Verwaltungspraxis festzuhalten, auch wenn diese im speziellen Beschwerdeverfahren nicht zum Tragen gekommen war.

Nach § 3 Abs. 1 StVG, § 46 Abs. 1 und 3 FeV hat die Fahrerlaubnisbehörde die Fahrerlaubnis zu entziehen, wenn sich jemand als ungeeignet zum Führen von Kraftfahrzeugen erweist. Bedenken an der Fahreignung sind durch Anordnung eines ärztlichen oder medizinisch-psychologischen Gutachtens aufzuklären (§§ 1 – 14 FeV). Dem Gutachter sind die von ihm benötigten Unterlagen zu übermitteln (§ 2 Abs. 14 Satz 1 StVG

i. V. m. § 11 Abs. 6 Satz 4 FeV). Wenn sich der Betroffene weigert, sich untersuchen zu lassen, oder das von der Fahrerlaubnisbehörde geforderte Gutachten nicht fristgerecht beibringt, darf die Fahrerlaubnisbehörde bei ihrer Entscheidung auf die Nichteignung schließen (§ 11 Abs. 8 Satz 1 FeV).

Somit existiert in § 2 Abs. 14 Satz 1 StVG eine gesetzliche Grundlage für die Übermittlung von Unterlagen an die MPU-Stelle. § 2 Abs. 14 Satz 1 StVG ist abschließend, so dass nur Unterlagen weitergegeben werden dürfen, die von der MPU-Stelle für die Erfüllung ihrer Aufgabe benötigt werden. Mit der Aufgabe ist der konkrete Untersuchungsauftrag gemeint. Diese Regelung korrespondiert mit der datenschutzrechtlichen Rechtsgrundlage und füllt somit den Begriff der Erforderlichkeit der Datenverarbeitung aus.

Die in § 2 Abs. 14 Satz 2 StVG erwähnte Verordnungsermächtigung bezieht sich ausdrücklich nur auf die Datenverarbeitungen durch die MPU-Stelle. Die daraufhin zu erlassende Rechtsverordnung soll eingrenzen, welche Daten die MPU-Stelle verarbeiten darf. Die in § 11 Abs. 6 Satz 4 FeV enthaltene Regelung der „Übersendung der vollständigen Unterlagen durch die Fahrerlaubnisbehörde“ ist daher im Lichte des § 2 Abs. 14 Satz 1 StVG in der Weise auszulegen, dass nur die benötigten Unterlagen, diese aber vollständig, übermittelt werden dürfen. Nicht benötigte Unterlagen unterfallen somit einem datenschutzrechtlichen Verwertungsverbot.

Bereits im IV. Tätigkeitsbericht des Landesbeauftragten für den Zeitraum vom 1. April 1997 bis 31. März 1999 (Nr. 27.2) ist die Befassung mit o. g. Thema anlässlich des Erlasses des neuen Fahrerlaubnisrechts und insbesondere der Fahrerlaubnisverordnung dokumentiert: „Der Landesbeauftragte begrüßt diese Regelung zur Datenverarbeitung, weist aber gleichzeitig daraufhin, dass eine vollständige normenklare Regelung nicht gelungen ist. Zwar wird die Datenübermittlung der Fahrerlaubnisbehörden an Stellen und Personen, welche die Eignung und Befähigung beurteilen oder prüfen, in § 2 Abs. 14 StVG geregelt. (…) Außerdem geht die FeV hinsichtlich der Übergabe der Unterlagen an die begutachtende Stelle über die Ermächtigungsnorm im StVG (§ 2 Abs. 14 Satz 1) hinaus. Während das StVG lediglich die Übermittlung der Daten vorsieht, die zur Aufgabenerfüllung benötigt werden, bestimmt die FeV (§ 11 Abs. 6 Satz 4) die Übersendung der vollständigen Unterlagen. Dies ist rechtlich unzulässig. Der Landesbeauftragte empfiehlt deshalb dem Ministerium für Wohnungswesen, Städtebau und Verkehr, bis zu einer Novellierung der FeV auf dem Erlasswege sicherzustellen, dass die Fahrerlaubnisbehörden regelmäßig die Akteneinsicht in diesen genannten Fällen anbieten und nur die erforderlichen Fahrerlaubnisunterlagen an die begutachtenden Stellen übersandt werden.“

Das zuständige Ministerium ist der damaligen Anregung des Landesbeauftragten nicht gefolgt. Das für die Aufsicht zuständige Landesverwaltungsamt sah auch im aktuellen Fall keinen Anlass, die Verwaltungspraxis der Führerscheinstelle aufsichtsbehördlich zu korrigieren.

9.2 Meldungen über Fahrverbote

Ein Beschwerdeführer wandte sich gegen die Unterrichtung der zuständigen Polizeidienststelle sowie der Fahrerlaubnisbehörde durch die Polizeiinspektion Zentrale Dienste Sachsen-Anhalt über ein ihn betreffendes Fahrverbot.

Hinsichtlich der Unterrichtung der Fahrerlaubnisbehörde berief sich die Polizeiinspektion auf einen Erlass des Ministeriums für Inneres und Sport (Runderlass des MI vom 25. Juni 1992, 21.1.05140-3/1 Ziff 9.5, zuletzt geändert am 23. Oktober 2007). Das daraufhin um Stellungnahme gebetene Ministerium für Inneres und Sport teilte mit, dass die Information der Fahrerlaubnisbehörden u. a. über Fahrverbote nach § 2 Abs. 12 Straßenverkehrsgesetz (StVG) unverzichtbar und für die Aufgabenerfüllung erforderlich sei.

Der Erlass des Ministeriums für Inneres und Sport sowie die Entscheidung der Zentralen Bußgeldstelle zur Datenübermittlung halten einer Überprüfung stand. Nach § 2 Abs. 12 StVG hat die Polizei Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist. Soweit die mitgeteilten Informationen für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten.

Es handelt sich hierbei um eine Informationspflicht der Polizei, soweit das Kriterium der Erforderlichkeit gegeben ist. Erforderlich ist eine Datenverarbeitung, wenn eine einzelfallbezogene Abwägung nach dem Verhältnismäßigkeitsprinzip zwischen der staatlich gewünschten Transparenz und dem Recht der betroffenen Personen auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen zugunsten der staatlichen Aufgabe ausfällt.

Bei der staatlichen Aufgabe handelt es sich um die Sicherheit des Verkehrs, sie obliegt sowohl der Polizei als auch der Fahrerlaubnisbehörde. Demnach darf die Polizei vor dem Hintergrund ihrer organisatorisch durch Aspekte der Verkehrssicherheit vorgeprägten Sichtweise entscheiden, ob eine Übermittlung erforderlich ist. Diese Entscheidung bedarf vorangehender Überlegungen im Einzelfall und würde bei pauschaler Handhabung gegen den Verhältnismäßigkeitsgrundsatz verstoßen.

Das zuständige Ministerium ist jedoch nicht gehindert, im Erlasswege für diese Einzelfallentscheidung Leitlinien aufzustellen. Nach der Gesetzesbegründung zum StVG sind neben Alkohol und Drogen auch Erkenntnisse zu einer andauernden Ungeeignetheit zum Führen von Fahrzeugen zu melden. Diese Vorgaben zeichnet der Erlass nach.

Unbedeutende Ordnungswidrigkeiten können keine Zweifel an z. B. der charakterlichen Eignung begründen, schwerwiegende Auffälligkeiten und grobe Pflichtverletzungen dagegen schon. Drei erhebliche Geschwindigkeitsüberschreitungen in kurzer Zeitfolge berechtigen die Fahrerlaubnisbehörde z. B. zur Anforderung eines medizinisch-psychologischen Gutachtens (VG München, Beschluss vom 20. Dezember 2006, M 1 S 06.4357 – juris).

Das Fahrverbot ist eine der einschneidensten Maßnahmen, die im Bußgeldkatalog verzeichnet sind. Ein Fahrverbot kann bei ganz unterschiedlichen Zuwiderhandlungen drohen. Grobe Verstöße, die regelmäßig mit zwei Punkten in Flensburg sanktioniert werden, ziehen meist ein Fahrverbot nach sich. Insoweit ist das Fahrverbot als Richtschnur zur Unterscheidung zwischen unerheblichen und schwerwiegenden Verstößen

tauglich. Hinsichtlich dieser Datenübermittlung war die Beschwerde also zurückzuweisen.

Die Polizeiinspektion Zentrale Dienste Sachsen-Anhalt teilte hinsichtlich der Datenübermittlung an die zuständige Polizeidienststelle mit, dass diese im Straßenverkehrsgesetz nicht vorgesehen und im Übrigen auch nicht erforderlich sei. Die Verfahrensweise der Zentralen Bußgeldstelle sei mit sofortiger Wirkung geändert worden. Insoweit war der Beschwerde stattzugeben.

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

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

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

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

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

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

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

Der Beschluss für die Akteneinsicht des Ortsbürgermeisters muss, auch wenn das Verfahren nicht eindeutig im Gesetzestext vorgeschrieben ist, wie auch der Beschluss zur Bildung eines Akteneinsichtsausschusses nach § 45 Abs. 6 KVG LSA, auf einen hinreichend konkreten Anlass bezogen sein. Das heißt, er muss auf einen Einzelfall

bzw. auf eine bestimmte Angelegenheit beschränkt sein (z. B. Verpachtung des Gemeindegrundstückes XY, nicht Untersuchung von Verpachtungen gemeindlicher Grundstücke allgemein, bzw. im konkreten Fall, nicht allgemein auf Parkverstöße im Bereich der Ortschaft). In den letztbenannten Fällen besteht die Gefahr, dass der Ortsbürgermeister durch solche Beschlüsse die Verwaltung dauerhaft kontrollieren würde, was nicht zu seinen Aufgaben gehört.

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

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

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

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

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

10 Verfassungsschutz

10.1 Verfassungsschutzgesetz

Am 21. Oktober 2020 ist das Gesetz zur Fortentwicklung des Verfassungsschutzes und der Sicherheitsüberprüfung im Land Sachsen-Anhalt in Kraft getreten. Der Landesbeauftragte hat im Rahmen des Gesetzgebungsverfahrens mehrfach zum Gesetzentwurf Stellung genommen, vgl. XVI. Tätigkeitsbericht (Kap. 9).

Der Landesbeauftragte hatte, mit Blick auf das bereits absehbar außer Kraft tretende DSG LSA, die Aufnahme eigener datenschutzrechtlicher Regelungen in das Verfassungsschutzgesetz des Landes empfohlen. Stattdessen entschied sich der Gesetzgeber für eine sogenannte „versteinerte Verweisung“. Danach verweist § 30 VerfSchG-LSA auf die einschlägigen Vorschriften des Datenschutzgesetzes Sachsen-Anhalt in der Fassung der Bekanntmachung vom 13. Januar 2016 bzw. in der Fassung vom

6. Mai 2018. Die Auffassung des Landesbeauftragten, dass eine solche Verweisung der Normenklarheit abträglich sein dürfte, wurde nicht geteilt.

Darüber hinaus wies der Landesbeauftragte darauf hin, dass die Erhebung und Speicherung von Daten Minderjähriger nach § 10 VerfSchG-LSA aus seiner Sicht unverhältnismäßig sein dürfte. Danach darf die Verfassungsschutzbehörde Daten über Minderjährige nach Vollendung des 14. und vor Vollendung des 16. Lebensjahres speichern, verändern und nutzen, wenn tatsächliche Anhaltspunkte für Bestrebungen vorliegen, eine Straftat nach dem Katalog des § 4 Abs. 1 VerfSchG-LSA zu begehen. § 4 Abs. 1 VerfSchG-LSA verweist ausschließlich auf Straftaten, die gegen die freiheitlich demokratische Grundordnung gerichtet sind. In der Gesetzesbegründung zu § 10 VerfSchG-LSA wird bei diesen Bestrebungen aber stets ein Bezug zu terroristischen Aktivitäten hergestellt, der sich aus dem Wortlaut des Gesetzes selbst nicht erschließt.

Weiterhin geht aus der Gesetzesbegründung hervor, dass noch erheblich weitergehende Eingriffe angestrebt werden. Mit dem Argument der möglichen Einflussnahme und Erziehung in Familien, die im extremistischen Bereich verhaftet sind, kann und soll ausweislich der Begründung jeder Minderjährige einer Familie in den Datenbanken des Verfassungsschutzes erfasst und gespeichert werden, wenn auch nur ein Elternteil extremistisch ist, da eine entsprechende Beeinflussung möglich sei. Eine eigene extremistische Betätigung der Minderjährigen verlangt weder die Regelung selbst noch die Gesetzesbegründung. Eine derart weitgehende „Mitverantwortung“ Minderjähriger für die Ansichten ihrer Eltern bei tatbestandlich sehr weitgehender Rechtslage verstößt aus Sicht des Landesbeauftragten sowohl gegen das Übermaßverbot als auch gegen das Bestimmtheitsgebot und ist damit rechtswidrig. Durch diese Regelung könnten auch Minderjährige, ohne dass sie sich selbst extremistisch betätigt hätten, als einem Extremismusbereich zugehörig gekennzeichnet werden.

11 Rechtspflege und Justizvollzug

11.1 Elektronischer Rechtsverkehr in der Justiz

Der Landesbeauftragte hat bereits in seinem XVI. Tätigkeitsbericht (Nr. 10.2) darüber informiert, dass an den Gerichten des Landes von einem „Elektronischen Rechtsverkehr“ keine Rede sein kann. Da die einzige im Projektzeitraum anberaumte Sitzung des Projektlenkungsausschusses des Ministeriums für Justiz und Gleichstellung aufgrund der Corona-Epidemie nicht zustande kam, ist zu befürchten, dass sich an dieser Situation auch aktuell nichts geändert hat.

11.2 Justiz-IT-Gesetz

Mit Stichtag zum 1. Januar 2026 muss die Digitalisierung in allen Gerichten und Staatsanwaltschaften des Landes umfassend vollzogen sein. Die Akten sind dann zwingend elektronisch zu führen. Zur Organisation und Umsetzung dieser Vorgaben wurde das Justiz-IT-Gesetz (JITG LSA) erlassen. Dieses regelt unter anderem die Einrichtung und Arbeitsweise eines IT-Kontrollbeirates mit umfassenden Kontroll- und Abhilferechten, die denen des Landesbeauftragten sehr ähnlich sind.

Während die Kompetenzverteilung für die Gerichte zunächst schlüssig erscheint, wirft sie für den Bereich der Staatsanwaltschaften hingegen Fragen auf. Nach der DS-GVO

bzw. der JI-Richtlinie können die Mitgliedstaaten vorsehen, neben Gerichten auch Staatsanwaltschaften im justiziellen Bereich von der Aufsichtszuständigkeit des Landesbeauftragten auszunehmen. Der Landesgesetzgeber hat sich jedoch sowohl im Rahmen der Umsetzung der JI-Richtlinie als auch bei der Ausfüllung der DS-GVO gegen diese Möglichkeit entschieden und den Landesbeauftragten uneingeschränkt zur Aufsichtsbehörde erklärt.

Das JITG LSA kollidiert hiermit, indem es Inhaltsdaten, welche die richterliche, rechtspflegerische oder staatsanwaltschaftliche Entscheidungsfindung ganz oder teilweise dokumentieren, einem besonderen Schutz unterwirft. Zudem räumt es dem IT-Kontrollbeirat das Recht ein, zum Zweck der Ausübung der Aufsichtstätigkeit, Einsicht in diese Daten zu nehmen.

Gleichzeitig beschränkt das Gesetz die aufsichtsrechtlichen Pflichten des IT-Kontrollbeirates auf den justiziellen Bereich der Gerichte. Diese Beschränkung wirft letztlich die Frage auf, weshalb die Staatsanwaltschaften zunächst so umfänglich in den Schutzbereich und in die Kontrollbefugnisse einbezogen wurden, wenn der IT-Kontrollbeirat aufsichtsrechtliche Pflichten nur gegenüber dem justiziellen Bereich der Gerichte auszuüben berechtigt ist.

Der Landesbeauftragte hat auf diesen Widerspruch im Rahmen seines Rechts zur Stellungnahme hingewiesen. Eine Berücksichtigung dieser Einwände erfolgte nicht. Inwieweit es in der Folge zwischen dem Landesbeauftragten und dem IT-Kontrollbeirat zu Differenzen hinsichtlich der Ausübung der datenschutzrechtlichen Aufsicht kommt, bleibt abzuwarten.

12 Schulwesen

12.1 Schuldatenschutz-Verordnung

Im XIII./XIV. Tätigkeitsbericht (Nr. 9.2.2) hatte der Landesbeauftragte dargestellt, dass die §§ 84a ff. SchulG LSA Verordnungsermächtigungen enthalten, von denen seit Ende 2012 kein Gebrauch gemacht wurde. Zur Erläuterung von gesetzlichen Begriffen, wie z. B. der „Schulpflichtmerkmale“, deren Inhalt und Bedeutung sich nur begrenzt erschließen, sowie zur Klärung von Verfahrensfragen im Hinblick auf die verschiedenen vorgesehenen digitalen Einrichtungen (z. B. zentrale Schülerdatei) besteht jedoch entsprechender Bedarf.

Nach umfangreichen Beratungen des Ministeriums für Bildung im Sommer 2016 zu einem Entwurf einer Schuldatenschutz-Verordnung wurde dieser zu inhaltlichen und technischen Abstimmungen in die Schulverwaltung übergeben. Ende 2019 erhielt der Landesbeauftragte sodann den Entwurf einer Verordnung über den Schutz personenbezogener Daten im Schulwesen des Landes Sachsen-Anhalt (SchulDatSchVO) zur Stellungnahme. Zur Vorbereitung einer Beratung konnte der Landesbeauftragte im Mai 2020 einen ausführlichen Vermerk an das Ministerium übersenden, in dem vielfache Hinweise zu datenschutzrechtlichen Optimierungen gegeben wurden. Ein Schwerpunkt war die Problematik der Nutzung privater Geräte, insbesondere von Smartpho-

nes und Tablets. Ein weiterer Schwerpunkt waren die Regelungen zu Statistiken. Daneben wurden vielfach Präzisierungsanregungen gegeben. Eine abschließende Beratung steht noch aus.

12.2 Datenschutzbeauftragte in Schulen

Seit 2012 verfolgt der Landesbeauftragte die bei Kontrollen und Stichproben festgestellte Problematik, dass an Schulen entgegen dem lange bestehenden gesetzlichen Gebot fast durchgängig keine behördlichen Datenschutzbeauftragten benannt sind. Seitdem besteht der Kontakt mit dem Ministerium für Bildung, um auf die Einhaltung der gesetzlichen Verpflichtungen hinzuwirken. Lösungsansätze, wie z. B. ein Ende 2014 abgestimmter Erlassentwurf wurden aber weiter administriert, siehe zur Entwicklung XI. Tätigkeitsbericht (Nr. 9.3.1), XII. Tätigkeitsbericht (Nr. 9.2.1) und XIII./XIV. Tätigkeitsbericht (Nr. 9.2.1). Zwischenzeitlich wurden vier Stellen im Landesschulamt vorgesehen, die dem Anliegen der Gewährleistung von Datenschutzbeauftragten an Schulen mit Rechnung tragen sollten. Zwei Mitarbeiter im Landesschulamt sind nun auch aktiv um die Problematik bemüht. Auch im Jahr 2020 ist jedoch noch keine abschließende Lösung für die seit weit über 10 Jahren andauernde Missachtung der gesetzlichen Vorgaben gegeben. Der Landesbeauftragte hat auch in diesem Jahr das Ministerium für Bildung und in verschiedenen Gesprächen die mit den Aufgaben betrauten Mitarbeiter im Landesschulamt beraten. Dabei ging es u. a. um viele kleine Schulen, die schwerlich einen Datenschutzbeauftragten aus den eigenen Reihen benennen können. Lösungen, wie gemeinsame Benennungen, die Berücksichtigung von externen Beauftragten und die Benennung von Beauftragten durch die Schulbehörde unter Einsatz von weiteren Kräften zur Unterstützung vor Ort, wurden diskutiert. Dazu wurde darauf hingewiesen, dass jeweils die Größe und die Organisationsstruktur der jeweils verantwortlichen Stellen nach Art. 37 Abs. 2 und 3 DS-GVO zu berücksichtigen sind. Wesentlich ist, dass eine persönliche Erreichbarkeit gewährleistet wird und der jeweils aktiven Person nur die Verantwortung für so viele Schulen übertragen wird, dass sie in der Lage ist, den Aufgabenbereich voll zu überblicken und die gesetzlichen Aufgaben in der zur Verfügung stehenden Zeit umfassend zu erledigen. Im Frühjahr 2021 hat das Landesschulamt nunmehr die beiden oben genannten Mitarbeiter als Datenschutzbeauftragte für die Schulen einmal für den Schulamtsbereich Nord und einmal für den Schulamtsbereich Süd benannt. Zusätzlich wurde den Schulen aufgegeben, für die Beauftragten jeweils einen Ansprechpartner zu benennen.

12.3 Handreichung „Datenschutz an Schulen“

Im XV. Tätigkeitsbericht (Nr. 10.2.1) hatte der Landesbeauftragte auf die Handreichung „Datenschutz an Schulen“ des Ministeriums für Bildung hingewiesen und erläutert, dass beabsichtigt ist, diese im Folgenden, soweit nötig, zu aktualisieren. Dazu hatte das Landesschulamt dem Landesbeauftragten einen Entwurf einer überarbeiteten Neufassung übersandt.

Der Landesbeauftragte hat das Landesschulamt umfänglich beraten und dabei neben redaktionellen Hinweisen zu vielen Themenkreisen Empfehlungen gegeben, wie z. B. zu Einwilligungserklärungen oder zur Problematik der behördlichen Datenschutzbeauftragten an Schulen. Ein Beratungsschwerpunkt waren die Regelungen zur Nutzung von privaten digitalen Geräten durch die Lehrkräfte. Der vorrangige Einsatz dienstlicher Geräte wurde im Hinblick darauf empfohlen, dass es der einzelnen Lehrkraft nur schwer möglich sein dürfte, die technischen und organisatorischen Anforderungen an

einen datenschutzkonformen zulässigen Betrieb (Art. 5 Abs. 1 lit. f, Art. 32 DS-GVO) zu gewährleisten. Insbesondere von der Nutzung von Smartphones und Tablets wurde abgeraten. Auf die Haftungsregelungen des Art. 82 DS-GVO wurde hingewiesen. Weiter ergingen umfängliche Empfehlungen, welche Hinweise die Schulverwaltung an die Schulleitungen zu Anforderungen in Bezug auf die Genehmigung der Nutzung privater Geräte geben kann.

Zu Auftragsverarbeitern wurde erläutert, dass diese gelegentlich Nutzerdaten auch für eigene Zwecke (Prozessoptimierung, Austausch mit Geschäftspartnern) verwenden. Infolge der Regelung des Art. 28 Abs. 10 DS-GVO wären sie damit als eigene Verantwortliche tätig (Art. 28 Abs. 10 DS-GVO), die Privilegierung der Auftragsverarbeitung ginge verloren und es läge somit eine Datenübermittlung an eigenständig Verantwortliche vor. Dies wäre aber bei privaten Anbietern nach § 84a Abs. 8 Satz 2 SchulG LSA in der Regel unzulässig. Ergänzend wurde begrüßt, dass die Nutzung landeseigener digitaler Technologie (Bildungsserver, emuCLOUD) im Vordergrund steht. So würde die Gefahr reduziert, dass durch die Nutzung von Programmanbietern eventuell mit Art. 44 ff. DS-GVO nicht kompatible Datenübermittlungen in Drittstaaten erfolgen.

12.4 Bildungsmanagementsystem

Zum Bildungsmanagementsystem hat der Landesbeauftragte das Ministerium für Bildung weiter beraten, siehe bereits XIII./XIV. Tätigkeitsbericht (Nr. 9.2.3) und XVI. Tätigkeitsbericht (Nr. 11.2.3). Dabei ging es insbesondere um die Maßnahmen zur Gewährleistung der Betroffenenrechte. Zu den seitens des Ministeriums entwickelten Entwürfen wurden zu verschiedenen Einzelpunkten Hinweise gegeben, um den Anforderungen der Art. 12 ff. DS-GVO Rechnung tragen zu können. Ein wesentlicher Punkt war zunächst die Klarstellung, wer Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO ist, unter Berücksichtigung der Frage nach einer gemeinsamen Verantwortlichkeit (Art. 26 DS-GVO). Das Ministerium für Bildung ist nach § 87f SchulG LSA Verantwortlicher für das Schulverwaltungsverfahren. Nach § 84c SchulG LSA richtet das Landesschulamt eine zentrale Schülerdatei ein, auf die beide Schulbehörden Zugriff haben. Auch nach § 5 Abs. 6 des Entwurfs einer SchulDatSchVO, der dem Landesbeauftragten vorlag, war ein Zugriff der Schulbehörden im Einzelfall vorgesehen. Nach § 84f SchulG LSA ist auch das Landesinstitut für Schulqualität und Lehrerbildung nutzungsberechtigt. Auch die Schulen sollen Schülerdaten mittels des landeseinheitlichen IT-gestützten Schulverwaltungssystems verarbeiten (§ 84c Abs. 1 Satz 6, § 84f Satz 2 SchulG LSA). Zur Ausgestaltung einer ggf. nach Art. 26 DS-GVO gebotenen vertraglichen Vereinbarung wurden verschiedene Möglichkeiten erörtert. Weiter wurden Hinweise zu Form und Umfang der Informationen nach Art. 13 DS-GVO, zu den Erläuterungen zur Herkunft der Daten und zur Art der Bereitstellung gegeben. Zum Auskunftsanspruch nach Art. 15 DS-GVO wurden Umfang und Geltendmachung erörtert. In technischer Hinsicht ging es u. a. um die Generierung von Testdaten, die aus zu verändernden Echtdatensätzen gewonnen werden sollten.

Aus Sicht des Datenschutzes wurde zum Zugriff auf das System betont, dass es vorzugswürdig erscheint, entsprechend der bisherigen Planungen für das Projekt Bildungsmanagement Schulbehörden nicht ohne Weiteres Zugriff auf sämtliche Schülerdaten zu gewähren (Vermeidung eines gläsernen Schülers). Die Begriffe „Zugriff“ in § 84c SchulG LSA und „Nutzung“ in § 84f SchulG LSA sollten so interpretiert werden, dass es bei der beabsichtigten Exportlösung bleibt, d. h., dass eine „Übermittlungshandlung“ der jeweils direkt verantwortlichen Schule vorgeschaltet ist (push statt pull).

12.5 Schul-Cloud des Hasso-Plattner-Instituts

Wie bereits im XVI. Tätigkeitsbericht (Nr. 11.2.4) erläutert, hat der Landesbeauftragte auch in diesem Berichtszeitraum die Beratungen der Schul-Cloud des Hasso-Plattner-Instituts (HPI) begleitet. Noch immer ungeklärt ist u. a. die Anbindung der Contentanbieter in der Cloud, um die Nutzer angemessen vor einem Tracking dieser Anbieter zu schützen.

Als Rechtsgrundlage für die Nutzung der Cloud kommt weiterhin ausschließlich die Einwilligung der Betroffenen in Betracht. Die Empfehlung des Landesbeauftragten, eine gesetzliche Grundlage im Schulgesetz zu ergänzen, die differenziert die Befugnisse für die Nutzung digitaler Techniken im Unterrichtsgeschehen ausgestaltet, ist bisher nicht umgesetzt worden.

Darüber hinaus wurden aufgrund anonymer Hinweise im März 2020 etliche Sicherheitslücken in der Schul-Cloud aufgedeckt. So konnte z. B. mit einer Einmal-E-Mail-Adresse ein Account in der Schul-Cloud eingerichtet werden, womit es mit wenig Aufwand möglich war, die Namen der angemeldeten Schüler einzusehen. Laut Mitteilung des HPI wurden die Sicherheitslücken unverzüglich geschlossen.

Die datenschutzrechtlichen Prüfungen hinsichtlich der grundsätzlich getroffenen technischen und organisatorischen Maßnahmen und der Sicherheitslücken sind noch nicht abgeschlossen. Infolge der ergänzenden finanziellen Mittel im Rahmen der Pandemiebekämpfung rückt auch die HPI-Schul-Cloud stärker in den Fokus. Der Landesbeauftragte wird die Entwicklung auch künftig begleiten.

12.6 Medienkompetenz

Die Digitalisierung hat durch die Corona-Pandemie in diesem Berichtszeitraum in vielen Lebensbereichen, vor allem auch in den Schulen, an Fahrt aufgenommen. Bereits seit vielen Jahren wirbt der Landesbeauftragte jedoch dafür, dass allein die technische Ausstattung von Schulen nicht ausreichend ist, sondern parallel auch digitale Bildung, d. h. die Vermittlung von Datenschutzbewusstsein und Medienkompetenz erfolgen muss. Das eine kann ohne das andere nicht funktionieren.

Die „Ländervereinbarung über die gemeinsame Verantwortung der Länder in zentralen bildungspolitischen Fragen“ sieht vor, dass die in der Strategie „Bildung in der digitalen Welt“ und dem DigitalPakt Schule vereinbarten Ziele konsequent weiterverfolgt werden. Diese sind u. a. die curriculare Verankerung der fachdidaktischen Kompetenzen zur Nutzung digitaler Medien in der Lehramtsausbildung und digitale Lehr- und Lernmittel für alle Fächer und Klassenstufen bis 2025. Dies wird vom Landesbeauftragten ausdrücklich begrüßt.

Der Bund wollte die Länder bei der Digitalisierung der Schulen mit insgesamt 6,5 Milliarden Euro unterstützen, u. a. für die Ausstattung der Lehrkräfte und von bedürftigen Kindern mit digitalen Endgeräten. Die Finanzierung erfolgt aus dem DigitalPakt Schule. Ferner dürfen die Schulen nunmehr Mittel aus dem DigitalPakt Schule abrufen, ohne dass zuvor ein pädagogisches Konzept vorgelegt werden muss. Darüber hinaus ist die Einrichtung von Kompetenzzentren für digitales und digital unterstütztes Unterrichten vorgesehen. Für die organisatorische und administrative Umsetzung des DigitalPakt Schule ist die „Landesinitiative für nachhaltige digitale Infrastrukturen für Unterricht und

Schule“ (LINDIUS) am LISA in Halle etabliert worden. Die Kompetenzzentren sollen die Schulen bei der Erstellung von Medienkonzepten und digitalen Schulentwicklungsplänen unterstützen. Auch soll der Bund eine übergreifende Bildungsplattform entwickeln, um die bereits bestehenden Systeme der Länder zu vernetzen. Der Landesbeauftragte wird die Fortentwicklung dieser Projekte weiterhin begleiten. In diesem Zusammenhang ist insbesondere darauf zu achten, dass die Schulen nicht zu digitalen Angeboten greifen, die aus datenschutzrechtlicher Sicht kritisch zu bewerten sind, da z. B. unzulässige Datenauswertungen des Nutzungsverhaltens durch Lehrkräfte oder die Softwareanbieter möglich sind.

Während die Landesarbeitsgemeinschaft „Medienbildung/Medienkompetenz“ in diesem Jahr überhaupt nicht getagt hat, hat der 5. Tag der Medienkompetenz Sachsen-Anhalt mit dem Fokus auf digitale Bildung virtuell mit vielen verschiedenen Angeboten stattgefunden.

12.7 Nachweis der Masernimpfung

Mit dem Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention (Masernschutzgesetz) trat am 1. März 2020 eine Masernimpfpflicht in Kraft. Damit verbunden ist eine Nachweispflicht in Bezug auf Impfschutz der in den gesetzlich festgelegten Gemeinschaftseinrichtungen (z. B. Kinderbetreuungseinrichtungen, Schulen) betreuten Personen und der in Gemeinschafts- und Gesundheitseinrichtungen tätigen Personen (z. B. Beschäftigte, Dienstleister, ehrenamtlich Tätige) gegenüber den Leitungen dieser Einrichtungen (§ 20 Absätze 9 bis 11 Infektionsschutzgesetz (IfSG)).

Aufgrund dieser Nachweispflicht erhielt der Landesbeauftragte in den folgenden Monaten zahlreiche telefonische und schriftliche Anfragen und Beschwerden besorgter Eltern. Teilweise wurden in den Schulen oder Kindertagesstätten ganze Impfausweise kopiert und zu den Akten genommen. Oft genügte es, den Eltern die Rechtslage zu erläutern. In einigen Fällen wurden die Schulen bzw. Kinderbetreuungseinrichtungen kontaktiert. Diese stellten ihr Verfahren nach einer entsprechenden Beratung um und vernichteten die gespeicherten Kopien der Impfausweise.

Nach § 20 Abs. 9 IfSG kommen folgende Nachweise in Betracht: ein Impfausweis, eine Impfbescheinigung, ein ärztliches Zeugnis, z. B. eine ärztliche Dokumentation über Gesundheitsuntersuchungen für Kinder und Jugendliche, aber auch ein ärztliches Zeugnis über Masernimmunität oder medizinische Kontraindikationen oder auch eine Bestätigung einer staatlichen Stelle oder anderen maßgeblichen Einrichtung, dass ein entsprechender Nachweis bereits vorgelegen hat.

Nach dem gesetzlichen Wortlaut ist der Nachweis vorzulegen. Damit genügen die Einsichtnahme durch die Einrichtungsleitung und der Vermerk in der Dokumentation der Einrichtung, dass der Nachweis vorgelegen hat. Hinweise darauf, dass die Regelung so zu verstehen sein könnte, dass eine Kopie des Nachweises bei der Einrichtung zu verbleiben hat, sind auch der Gesetzesbegründung nicht zu entnehmen.

Die Aufnahme von ungeschwärzten Kopien von Impfausweisen begründet zudem die Gefahr, dass weitere medizinische Informationen gespeichert werden. Um nicht gegen das Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) zu verstoßen, ist daher vom Anfertigen und Abspeichern von Impfausweiskopien grundsätzlich abzusehen.

12.8 Fotokopien von Prüfungsunterlagen

In Prüfungsordnungen bzw. -gesetzen finden sich vielfach Regelungen, die den Zugang des Kandidaten zu seinen Prüfungsarbeiten auf das Einsichtsrecht beschränken und zeitlich befristen. In einem Beschwerdevorgang hatte eine Schule die Übersendung von Fotokopien von Abiturprüfungsarbeiten mit dem Hinweis auf das durch Erlass lediglich erlaubte Einsichtsrecht abgelehnt.

Beantragt ein Prüfungskandidat ausdrücklich Auskunft oder ist sein Antrag bei verständiger Würdigung durch die zuständige Behörde dahin auszulegen, besteht ein Auskunftsanspruch. Werden Fotokopien gewünscht, ist dieses Anliegen so zu interpretieren, dass der Betroffene seine Rechte dahin ausüben will, dass ihm seine Prüfungsantworten und die bewertenden Anmerkungen der Prüfer in verkörperter Form zur Verfügung gestellt werden.

Ein derartiger Anspruch ergibt sich für den Betroffenen aus dem Auskunftsanspruch der DS-GVO. Auch wenn die Prüfungsarbeiten in Papierform abgeheftet sind, ist die Anwendbarkeit der DS-GVO gegeben, da davon auszugehen ist, dass die Vorgänge in einem Dateisystem gespeichert sind (Art. 2 Abs. 1 DS-GVO). Über § 3 Abs. 2 Satz 1 Nr. 3 DSAG LSA wäre sie zumindest entsprechend anwendbar. Art. 15 Abs. 1 DS-GVO gewährt den betroffenen Personen ein Recht auf Auskunft zu den zu ihnen gespeicherten personenbezogenen Daten. Nach der Entscheidung des EuGH vom 20. Dezember 2017 (Az.: C 434/16[32]) handelt es sich bei Prüfungsantworten und etwaigen Anmerkungen der Prüfer um personenbezogene Daten des Prüfungskandidaten. Die Auskunft bezieht sich auf diese Daten. Weiter gewährt Art. 15 Abs. 3 DS-GVO ein Recht auf eine Kopie.

Auch wenn der Begriff „Kopie“ auslegungsfähig erscheint, dürfte zumindest bei Prüfungsarbeiten in Papierform kaum eine andere Form der Kopie als durch Fotokopie bzw. Scan möglich sein. Dieser Anspruch besteht unentgeltlich und zeitlich unbeschränkt. Lediglich für „weitere“ Kopien kann der Verantwortliche ein Entgelt verlangen.

Ausnahmen zu diesem Recht sieht Art. 15 DS-GVO selbst nicht vor. Einschränkungen können zwar auf gesetzlicher Basis erfolgen. Die jeweilige Regelung müsste dann aber den Anforderungen des Art. 23 DS-GVO entsprechen, was für die herkömmlichen einschränkenden Regelungen in Prüfungsordnungen bzw. -gesetzen in der Regel nicht zutreffen dürfte. Bei Prüfungsarbeiten sind auch nicht die Voraussetzungen der Einschränkung des Auskunftsrechts nach § 11 DSAG LSA gegeben.

Der Landesbeauftragte hat die Problematik mit einigen Ministerien erörtert und für dieses Thema sensibilisiert.

Prüfungskandidaten haben grundsätzlich einen unbefristeten Anspruch auf eine unentgeltliche Kopie ihrer Prüfungsunterlagen einschließlich der Bewertungen der Prüfer.

[32] https://curia.europa.eu/juris/document/document.jsf?docid=198059&doclang=DE

12.9 Datenübermittlung an den freien Schulträger

Ein Schüler einer Grundschule in freier Trägerschaft war von seinem Vater mündlich von der Schule abgemeldet worden. Am Folgetag erschien der Schüler nicht zur schulärztlichen Untersuchung. Die Ärztin des Gesundheitsamtes hatte auch keine Unterlagen zu dem Schüler, was von ihr und der Schule als besorgniserregend angesehen wurde. Die stellvertretende Schulleitung hat daraufhin ein Vorstandsmitglied des Trägers der freien Schule informiert, das kurze Zeit später ohnehin die Schulleitung übernehmen sollte. Das Vorstandsmitglied wurde über Namen, Fehlzeiten, Auffälligkeiten sozial-emotionaler Natur, Pflegeverhältnis, ungesundes und ungezügeltes Essverhalten, Übergewicht und die mündliche Kündigung des Schulvertrages informiert. Da die Eltern auf eine Einladung zum Gespräch nicht reagierten und die Teilnahme an der Schulreihenuntersuchung in Frage stand, hatte die Ärztin des Gesundheitsamtes angeregt, die entsprechenden Ämter zu informieren. Die Vorstandsvorsitzende des Trägervereins informierte sodann unter der wahrheitswidrigen Behauptung, sie sei Lehrerin an der Grundschule, das Schulamt, das Jugendamt und das Gesundheitsamt des Nachbarlandkreises, in dem der Schüler wohnte. Die Eltern waren über die Datenflüsse erbost und wandten sich an den Landesbeauftragten.

Der Landesbeauftragte wies die Schule auf die Problematik der Übermittlung sensibler Daten durch die Schule an das Vorstandsmitglied des Trägervereins hin und bat um Stellungnahme. Die Antwort kam sodann nicht von der Schule als datenschutzrechtlich Verantwortliche, sondern von der Vorsitzenden des Trägervereins. Das Vorstandsmitglied habe in Erfüllung von Aufgaben des Schulträgers gehandelt, um die Teilnahme an Schuluntersuchungen zu befördern. Dazu wurde die Schule als Verantwortliche darauf hingewiesen, dass zwar die Privatschulfreiheit inhaltlichen Einfluss gewährt. Dennoch ist zwischen der Trägerschaft der Schule (Einrichtung, Personal- und Sachmittel) und der Schule in ihren erzieherischen Belangen zu trennen. Auch der bei freien Schulen mögliche inhaltliche Einfluss bedeutet nicht, dass die klaren gesetzlichen Vorgaben der Datenverarbeitung nach § 84a SchulG LSA für Schulen in freier Trägerschaft eingeschränkt wären (§ 84a Abs. 13 SchulG LSA). Nach der Satzung betreibt der Verein neben der Schule auch andere Einrichtungen, wie etwa im Bereich der Kinder- und Jugendarbeit. Er ist datenschutzrechtlich als anderer Verantwortlicher anzusehen. Auch das Schulgesetz differenziert in § 16a SchulG LSA zwischen Schulträger und Schule. Daher ist die Schule Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO, der darüber hinaus wirkende Verein und seine Organe sind dagegen Dritte (Art. 4 Nr. 10 DS-GVO). Diese Auffassung hat der Landesbeauftragte mit dem Ministerium für Bildung des Landes Sachsen-Anhalt erörtert, das diese Auffassung teilt.

Der Rechtsanwalt der Schule bzw. des Trägervereins vertrat sodann die Meinung, die Schulleitung stehe arbeitsrechtlich-hierarchisch unterhalb des Vorstands. Nach zivil- und arbeitsrechtlichen Grundsätzen falle die datenschutzrechtliche Verantwortlichkeit dem Träger zu. Der Landesbeauftragte ergänzte dazu, dass die Schule infolge ihrer schulrechtlichen Ausgestaltung eine derart verselbständigte Einrichtung ist, dass sie selbst über Zwecke und Mittel der Verarbeitung entscheidet, auch wenn der Träger sie ausstattet. Maßstab für den Umgang mit schulischen Daten aus der Erziehungs- und Bildungsarbeit der Schule ist das Schulgesetz. § 84a Abs. 8 SchulG LSA, der nach Abs. 13 auf die Schule in freier Trägerschaft Anwendung findet, gestattet grundsätzlich keine Übermittlung von Daten aus dem Schulbetrieb zu Schülerinnen und Schüler an nichtöffentliche Dritte, es sei denn, die Übermittlung ist zur Rechtsverfolgung insbe-

sondere für Ersatzansprüche erforderlich und überwiegt das Geheimhaltungsinteresse. In weiterer Korrespondenz blieb der Rechtsanwalt der Schule bzw. des Trägervereins bei der Auffassung, das Vorstandsmitglied sei vertretungsberechtigtes Organ der Schule. Unabhängig von der wirtschaftlichen Verflechtung bleibt aber schulgesetzlich und datenschutzrechtlich die amtierende Schulleitung für den datenschutzkonformen Umgang mit sensiblen Schülerdaten verantwortlich. Da das Vorstandsmitglied des Vereins inzwischen Lehrerin und Schulleiterin der freien Schule geworden war, begründete dies die Gefahr, dass auch künftig mit der rechtswidrigen Übermittlung von personenbezogenen Daten von Schülerinnen und Schülern aus dem pädagogischen und verwaltungsmäßigen Schulbetrieb an den Trägerverein gerechnet werden musste. Im Interesse des Schutzes der Persönlichkeitsrechte der Schülerinnen und Schüler war es daher geboten, mittels Verwarnung gegenüber der Schule als Maßnahme nach Art. 58 Abs. 2 lit. b DS-GVO festzustellen, dass die Übermittlung der Daten zu dem Schüler (Fehlzeiten, Auffälligkeiten sozial-emotionaler Natur, ungesundes und ungezügeltes Essverhalten, Übergewicht) an die Vorsitzende des Trägervereins unzulässig war und die Aufsichtsbehörde hierüber in Kenntnis zu setzen.

13 Corona-Pandemie

13.1 Datenschutz gilt auch während der Corona-Pandemie

Die Corona-Pandemie prägte den Datenschutz im Jahr 2020. Mit der Ausbreitung des Virus und der notwendigen Maßnahmen zur Eindämmung der Pandemie traten schnell vielfältige datenschutzrelevante Fragestellungen auf. Dies betraf u. a. Fragen zur Gesundheit und zu Kontakten gegenüber Beschäftigten und Gästen, den Umgang mit den Daten der Infizierten, die Datenerhebungen im Zusammenhang mit vorbeugenden Maßnahmen sowie Fragen zur Heimarbeit und zum Fernunterricht. Die Bewältigung der Corona-Pandemie forderte von staatlichen Akteuren in der Legislative und der Exekutive, Maßnahmen vorzugeben und umzusetzen, die in erheblichem Umfang verschiedene Grundrechte der Bürgerinnen und Bürger betraf. Die Notwendigkeiten zum Schutz von Leben und Gesundheit der Bevölkerung müssen aber jeweils mit den Grund- und Freiheitsrechten der Bürgerinnen und Bürger in Einklang gebracht werden. Die Beachtung rechtsstaatlicher Vorgaben garantiert dabei die Stabilität von Staat und Gesellschaft. In Bezug auf den Schutz personenbezogener Daten sind europaweit einheitliche Grundsätze vorgegeben, die gerade in Krisenzeiten als Leitfaden für staatliches Handeln weiterhin Geltung beanspruchen. Darauf wies die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. April 2020 hin („Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie“, **Anlage 1**). Der Landesbeauftragte hat neben umfänglichen schriftlichen und telefonischen Beratungen auch allgemeine und spezifische Hinweise zum Datenschutz im Zusammenhang mit der Corona-Pandemie auf seiner Homepage veröffentlicht.

13.2 Fragen an Beschäftigte und Besucher

In den ersten Fragestellungen im Zusammenhang mit Eindämmungsmaßnahmen ging es um die Zulässigkeit von Erhebungen durch Arbeitgeber und Dienstherren gegenüber Beschäftigten und Besuchern. Dabei war zu berücksichtigen, dass zu erhebende

Daten in Bezug auf die Gesundheit zu den nach Art. 9 DS-GVO geschützten besonderen Kategorien von Daten zählen. Vorrangig ging es um Informationen darüber, ob bei der betroffenen Person eine Infektion festgestellt wurde oder ob Kontakt mit einer nachweislich infizierten Person bestanden hat. Weiter interessierte, ob kurz zuvor ein Aufenthalt in einem vom Robert-Koch-Institut als Risikogebiet eingestuften Gebiet stattgefunden hat. Dazu wurde darauf hingewiesen, dass sich diese Maßnahmen rechtlich auf Grundlage der DS-GVO und des BDSG sowie ggf. Landesdatenschutz- und weiteren Fachgesetzen legitimieren ließen. Die Berechtigung zur Verarbeitung personenbezogener Beschäftigtendaten ergibt sich in diesen Fällen für öffentlich-rechtliche Arbeitgeber grundsätzlich aus Art. 6 Abs. 1 Satz 1 lit. e DS-GVO, § 50 Satz 4 BeamtStG und § 84 Abs. 1 LBG LSA (ggf. i. V. m. § 26 Abs. 1 DSAG LSA) und für Arbeitgeber im nichtöffentlichen Bereich aus § 26 Abs 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Soweit Gesundheitsdaten verarbeitet werden, sind zudem auch § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DS-GVO einschlägig. Bei Art. 9 Abs. 2 lit. b DS-GVO umfasst der Begriff „Arbeitsrecht“ nach Auffassung der Datenschutzaufsichtsbehörden auch das deutsche Beamtenrecht. Zugunsten des öffentlich-rechtlichen Arbeitgebers könnte zusätzlich Art. 9 Abs. 2 lit. g DS-GVO herangezogen werden, da die Fürsorgepflicht im Sinne der Gesundheitsvorsorge hier auch einem wichtigen öffentlichen Interesse dient.

13.3 Fieberkurve der Mitarbeiter

Durch eine Eingabe erfuhr der Landesbeauftragte, dass ein Gesundheitsamt im April 2020 alle Schulen in seinem Zuständigkeitsbereich aufgefordert hatte, von den Beschäftigten einen Fragebogen mit Zeilen für jeden Tag ausfüllen zu lassen, der zulässige Fragen nach spezifischen Krankheitssymptomen, Kontakt zu Infizierten und zur Rückkehr aus Risikogebieten enthielt. Dazu sollte jeden Tag in der Schule die Körpertemperatur gemessen und eingetragen werden. Der Fragebogen sollte dann 4 Wochen in der Schule aufbewahrt werden.

Es war nachvollziehbar, dass im Zusammenhang mit der Vielzahl von Problemen bei Wiederaufnahme des Schulbetriebs begleitende Hinweise und ggf. Maßnahmen geboten erschienen. Aus datenschutzrechtlicher Sicht bestanden allerdings gegen die beabsichtigten listenmäßigen Erfassungen von Fieberdaten in den Schulen erhebliche Bedenken. Maßnahmen zum Schutz von Leben und Gesundheit der Bevölkerung sind mit den Grund- und Freiheitsrechten der Bürgerinnen und Bürger in Einklang zu bringen. Europarechtliche Datenschutzgrundsätze sind zu beachten. Vornehmlich zu berücksichtigen waren der besondere Schutz von Fieberdaten als Gesundheitsdaten (Art. 9 DS-GVO) und die Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 lit. b, c und e DS-GVO). Staatliches Handeln bleibt auch nach der DS-GVO vom Grundsatz der Erforderlichkeit geprägt.

Danach erschien es nicht zulässig, dass Arbeitgeber von ihren Beschäftigten Fieberdaten erfassen, aufzeichnen und speichern (Fieberkurve). Es würden alle Beschäftigten erfasst, unabhängig davon, ob im Einzelfall ein Anlass besteht. Die Geeignetheit der Erfassung und Speicherung der Fieberkurve erschien fraglich. Zunächst dürfte es eine Vielzahl von Fieberfällen geben, die nicht durch eine SARS-CoV-2-Infektion verursacht sind. Eine messbar erhöhte Temperatur muss nicht einmal stets auf einer Krankheit beruhen (z. B. Schlange stehen in der Sonne, Anfahrt mit dem Rad etc.). Auch ist eine erhöhte Körpertemperatur nicht zwingend symptomatisch für eine Covid-19-Infektion. So hatte das Robert-Koch-Institut im April 2020 im Steckbrief zur SARS-

CoV-2-Infektion mitgeteilt, dass in Deutschland lediglich 42% der Infizierten Fiebersymptome aufweisen. Auch die Erforderlichkeit war fraglich. Geht es darum, bei Erkenntnissen über einen konkreten Infektionsfall die Kontaktpersonen ausfindig zu machen, dürften Anwesenheitslisten ausreichen. Geht es darum, Personen mit erhöhter Temperatur auszusondern, käme als milderes Mittel in Betracht, die Beschäftigten aufzufordern, selbst zuhause bei Verdacht Fieber zu messen und bei erhöhter Temperatur vom Schulbesuch abzusehen. Es war nicht anzunehmen, dass die Beschäftigten gerade zu Beginn der Krisensituation dem nicht Folge leisten würden, sodass eine regelmäßige Kontrolle vor Ort geboten wäre.

Dem Anliegen des Gesundheitsamtes standen die Persönlichkeitsrechte der Betroffenen entgegen. Dabei war zu berücksichtigen, dass sich der Grundrechtseingriff mit der Vielzahl der erhobenen sensiblen Daten erhöht, wobei fast alle als Gesunde betroffen sind. Die zwangsweise Erhebung von sensiblen Gesundheitsdaten darf nur erfolgen, wenn dies für die Erreichung eines überragenden Zieles unerlässlich ist. Die 4-wöchige Speicherung (Fieberkurve) stellte einen erheblichen Eingriff in das Persönlichkeitsrecht insbesondere in Bezug auf weibliche Beschäftigte dar. Auch die Verhältnismäßigkeit erschien daher mit Blick auf die milderen Mittel, die ähnliche Resultate bewirken könnten, fraglich. Im Ergebnis der Beratung hat das Gesundheitsamt sodann auf die Erfassung und Speicherung von Fieberdaten verzichtet.

13.4 Wärmebildkameras

Da eine SARS-CoV-2-Infektion teilweise mit einer erhöhten Körpertemperatur einhergeht, werden zunehmend elektronische Geräte zur Temperaturerfassung als Mittel der Zutrittssteuerung eingesetzt. Eine kontaktlose Temperaturmessung erfolgt in der Regel per Infrarotmessung und wird entweder mithilfe eines Fieberthermometers oder einer Thermalkamera- bzw. Wärmebildkamera vorgenommen. Die Nutzung von Wärmebildkameras wird insbesondere in großen Einrichtungen in Betracht gezogen, da mittels klassischer Fieberthermometer keine Temperaturmessung bei größeren Gruppen erfolgen kann. Informationen zur Zulässigkeit der Erfassung einer gesteigerten Körpertemperatur bei Gästen, Kunden bzw. Besuchern wurde häufig nachgefragt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fasste dazu am 10. September 2020 den Beschluss „Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie“. [33] Darin sind einige grundsätzlich denkbare Rechtsgrundlagen dargestellt worden. Jedoch fehlt es in der Regel an der Eignung und der Erforderlichkeit der Messung. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden, und viele Infizierte weisen keine Symptome und damit auch keine erhöhte Temperatur auf. Zudem sind mildere Maßnahmen wie z. B. die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der Beschäftigten durch den Arbeitgeber denkbar. Demgemäß begegnet die Nutzung von Wärmebildkameras in der Regel durchgreifenden datenschutzrechtlichen Bedenken.

[33] https://lsaurl.de/DSKWaermebildkameras

13.5 Listen von Personen in Quarantäne

Aufgrund von gesetzlichen Meldepflichten sind die Gesundheitsämter über diejenigen Personen informiert, bei denen eine SARS-CoV-2-Infektion positiv festgestellt wurde. Dies führte zu Anordnungen von Quarantänemaßnahmen gegenüber den Infizierten sowie gegenüber Kontaktpersonen. An den diesbezüglichen Erkenntnissen bestand ein reges Interesse, u. a., um mittels Betroffenenlisten Quarantäneeinhaltungen zu prüfen und um Personen, die aus beruflichen Gründen andere Personen zu Hause aufsuchen müssen (Polizei, Rettungsdienste, etc.) über ggf. bestehende Infektionsgefahren vorab zu informieren. So wurde der Landesbeauftragte darüber informiert, dass Gesundheitsämter seitens des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt dazu aufgefordert worden waren, Betroffenenlisten mit Daten zu Personen in Quarantäne mit Anschrift und weiteren Daten zu übermitteln. Dazu hat der Landesbeauftragte umgehend das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt sowie das Ministerium für Arbeit, Soziales und Integration des Landes Sachsen-Anhalt auf die grundsätzliche Unzulässigkeit derartiger Übermittlungen und die ggf. notwendige Löschung bereits übermittelter Daten hingewiesen.

Die Maßnahmen zur Verhütung und Bekämpfung von auf Menschen übertragbaren Krankheiten obliegen den kommunalen und staatlichen Trägern des öffentlichen Gesundheitsdienstes. Diesen ist die Übermittlung von personenbezogenen Daten nach § 24 Abs. 1 Nr. 3 i. V. m. § 23 Abs. 2 Nr. 3 GDG LSA gestattet, wenn dies zur Abwehr einer Gefahr für Leben, Gesundheit oder Freiheit von Betroffenen oder Dritten erforderlich ist und die Gefahr nicht auf andere Weise beseitigt werden kann. Diese Voraussetzungen waren nicht erfüllt. Es waren keine Anhaltspunkte dafür bekannt, dass Personen, die über ihre Erkrankung informiert wurden und Quarantänevorgaben zu beachten hatten, dem nicht folgen würden. So bestätigte ein Landkreis, dass sich die betroffenen Personen an die Quarantänevorgaben halten. Für eine hinreichende Wahrscheinlichkeit der Verletzung der Gesundheit oder des Lebens anderer Personen, die ein Einschreiten der Polizei über die Kontrollaufgaben der Gesundheitsämter hinaus erforderlich gemacht hätte, lagen keine ausreichenden lokalen Hinweise vor. Erst wenn das zuständige Gesundheitsamt zum Schluss gekommen wäre, dass Überprüfungen der Quarantänemaßnahmen in größerem Umfang unumgänglich sind und die lokalen Kapazitäten dafür nicht ausreichen, wäre die Bitte der Polizei des Landes Sachsen-Anhalt um Unterstützung vertretbar gewesen. Zudem setzt eine zulässige Übermittlung nach § 24 Abs. 1 Nr. 3 i. V. m. § 23 Abs. 2 Nr. 3 GDG LSA voraus, dass sie geeignet, erforderlich und verhältnismäßig im engeren Sinne ist. Insoweit bestanden erhebliche Zweifel. Da sich aus fachlicher Sicht wohl fast alle regelkonform verhielten, erschien eine pauschale Kontrolle aller Betroffenen unverhältnismäßig. Zudem hätte die vorgesehene Verarbeitung stigmatisierend gewirkt.

Auch eine Übermittlung der Daten unter dem Aspekt des Schutzes der Beschäftigten vor Ansteckungsgefahr begegnete in Bezug auf die Polizei des Landes Sachsen-Anhalt und auch auf Rettungsdienste, die sich um diese Daten bemühten, erheblichen Bedenken. Hier war eine Übermittlung ebenfalls nicht erforderlich. Der Schutz der Beschäftigten wird nur in geringem Umfang bewirkt. Der Selbstschutz bleibt stets weiter geboten, zumal wohl der weitaus größte Teil der Infizierten mangels umfassender, flächendeckender Testung ohnehin nicht registriert ist. Auch wären von einer solchen Übermittlung alle von der Quarantäne betroffenen Personen erfasst, obwohl keine oder nur einige wenige von ihnen während der Zeit der Ansteckungsgefahr mit der Polizei des Landes Sachsen-Anhalt oder mit dem Rettungsdienst in Kontakt kommen.

Weiter waren für die Betroffenen weniger beeinträchtigende Maßnahmen denkbar (hinreichende Selbstschutzmaßnahmen, wie z. B. Masken). Insgesamt war deshalb von einer grundsätzlich unzulässigen Vorratsdatenspeicherung abzusehen.

Das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt hat die umfassende Abfrage der Daten umgehend zurückgezogen. Das Ministerium für Arbeit, Soziales und Integration des Landes Sachsen-Anhalt hat die Bedenken des Landesbeauftragten gegen die Übermittlung von Listen von Infizierten bzw. Personen in Quarantäne an Rettungsdienste geteilt und dies in einer Beratung mit den Leitern der Gesundheitsämter vermittelt.

13.6 Kontaktdatenerfassung

Die Maßnahmen zur Bekämpfung der Corona-Pandemie auf der Basis des Infektionsschutzgesetzes machten es bei der Durchführung von Veranstaltungen in Gaststätten und in anderen Einrichtungen erforderlich, Kontaktdaten von Besuchern bzw. Kunden zu erfassen. Die Vorgaben zur Erfassung ergaben sich aus den Verordnungen und Verfügungen der Gesundheitsbehörden auf Basis des Infektionsschutzgesetzes. In Bezug auf die Umsetzung gingen beim Landesbeauftragten Beschwerden und Anfragen ein. Der Landesbeauftragte hat daher auf der Homepage die „Hinweise zur Kontaktdatenerfassung bei der Corona-Bekämpfung“[34] aufgenommen. Darin wurde u. a. dargestellt, dass nur die durch die Verordnung oder die Verfügung der Gesundheitsbehörde vorgegebenen Daten erfasst werden dürfen und die Vertraulichkeit zu wahren ist (kein Auslegen von einsehbaren Listen, keine längere Speicherung als erforderlich, taggenaue Prüfung, ob eine Löschung geboten ist). Weiter wurde auf die enge Zweckbindung der Datenverarbeitung hingewiesen.

13.7 Mund-Nasen-Bedeckung

Die SARS-CoV-2-Eindämmungsverordnung sieht in bestimmten Situationen das Tragen einer Mund-Nasen-Bedeckung verpflichtend vor. Ausnahmen davon sind u. a. vorgesehen für Personen, denen die Verwendung einer Mund-Nasen-Bedeckung aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist; dies ist in geeigneter Weise (z. B. durch plausible mündliche Erklärung, Schwerbehindertenausweis, ärztliche Bescheinigung) glaubhaft zu machen (vgl. z. B. § 1 Abs. 2 Satz 2 der 8. SARS-CoV-2-EindV). Glaubhaftmachung ist mehr als eine Behauptung, verlangt jedoch keinen „Vollbeweis“. Dies kann auch durch Vorlage einer ärztlichen Bescheinigung erfolgen, insbesondere zur Vermeidung der Offenbarung von besonders geschützten Gesundheitsinformationen. Hierzu veröffentlichte der Landesbeauftragte die „Hinweise zur Befreiung von der Pflicht zum Tragen von Mund-Nasen-Bedeckungen“ auf der Homepage.[35]

Ob die Verwendung einer Mund-Nasen-Bedeckung aus gesundheitlichen Gründen unzumutbar oder nicht möglich ist, ist als medizinische Frage in die Bewertung des Arztes gestellt. Entgegen der Auffassung einiger gerichtlicher Entscheidungen in anderen Ländern erscheint das Anfordern von näheren Begründungen oder gar Diagnosen bei

[34] https://lsaurl.de/Kontaktdatenerfassung

[35] https://lsaurl.de/NoMask

Vorlage eines ärztlichen Attests in der Regel weder geeignet noch erforderlich (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Gelegentlich geltend gemachte Bedenken wegen möglicher Bescheinigungen aus Gefälligkeit bzw. aus dem Internet waren zwar nachvollziehbar. Die Erhebung einzelner Gesundheitsdaten über die ärztliche Feststellung hinaus ist grundsätzlich jedoch nicht geboten. Die Abfrage weiterer medizinischer Informationen ist nicht geeignet, da dies kurzfristig dazu führen würde, dass auch Bescheinigungen aus Gefälligkeit bzw. aus dem Internet derartige Daten aufführen. Bei begründetem Zweifel kann man im besonderen Einzelfall ein amtsärztliches Attest als milderes Mittel verlangen. Bei flüchtigen Zugangskontrollen erscheint es auch nicht praktikabel, medizinische Details oder gar Diagnosen zu prüfen. Auch der Text und die Begründung der Verordnung sprechen dafür, die Anforderungen niedrigschwellig anzusetzen. Ein erheblicher Grundrechtseingriff durch Abfrage sensibler medizinischer Informationen ist daher in der Regel nicht gerechtfertigt. Ergänzend wurde darauf hingewiesen, dass die Anfertigung und Speicherung von Kopien von ärztlichen Bescheinigungen bzw. die Speicherung von Originalen in der Regel nicht erforderlich und damit unzulässig ist (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Zu Dokumentationszwecken reicht ein Vermerk aus, dass die Ausnahme durch ärztliche Bescheinigung glaubhaft gemacht wurde.

13.8 Nutzung von Kontaktlisten für die Strafverfolgung

Aufgrund der Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in der Bundesrepublik Deutschland waren Restaurants, Gaststätten und andere Einrichtungen aufgefordert, alle Gäste bzw. Besucher mit Hilfe von Anwesenheitsnachweisen zu registrieren. Diese Maßnahme sollte im Falle einer auftretenden Infektion die Information möglicher infizierter Personen sicherstellen.

Mit verschiedenen Presseberichten wurde darauf hingewiesen, dass es bundesweit in einigen Fällen zur Einsichtnahme in diese Anwesenheitsnachweise durch die Polizei kam, um so Zeugen für im fraglichen Zeitraum verzeichnete Straftaten zu ermitteln.

Der Landesbeauftragte nahm diese Informationen zum Anlass und bat das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt um Auskunft, ob die hiesige Polizei ebenso verfahre und auf welcher Rechtsgrundlage dies stattfinde.

Das Ministerium führte aus, dass bis zum Zeitpunkt der Anfrage keine entsprechenden Vorgänge bei der Polizei des Landes Sachsen-Anhalt zu verzeichnen waren. Gleichwohl wies das Ministerium auf die nach Strafprozessordnung bundesweit bestehende Rechtslage hin, wonach die Polizei als Ermittlungsperson der Staatsanwaltschaft im Zuge der Strafverfolgung berechtigt und verpflichtet ist, Beweismaterial sicherzustellen, wenn es zur Aufklärung einer Straftat dienen kann.

Mit Wirkung vom 19. November 2020 wurde der § 28a des Infektionsschutzgesetzes ergänzt. Dieser schließt nunmehr in Abs. 4 Satz 3 die Verwendung der Anwesenheitsnachweise zu einem anderen Zweck als der Kontaktnachverfolgung aus.

Anwesenheitsnachweise, welche aus Anlass der Coronapandemie erstellt wurden, dürfen ausschließlich zur Kontaktnachverfolgung durch die zuständigen Stellen verwendet werden.

14 Gesundheits- und Sozialwesen

14.1 Gesundheitswesen

14.1.1 Aufzeichnungen der Rettungsleitstelle

Nach § 20 Abs. 2 Satz 1 RettDG LSA ist die Sprach- und Datenkommunikation der Rettungsdienstleitstellen durchgehend zu dokumentieren. Aus dem Rettungsdienst eines Landkreises erhielt der Landesbeauftragte eine Anfrage und eine Beschwerde zur Zulässigkeit des Abhörens der Aufzeichnungen. Es werde sogar eine Amtsnummer abgehört. Auf Nachfrage teilte der Ärztliche Leiter des Rettungsdienstes zunächst mit, dass lediglich einzelne Aufzeichnungen unter qualitätssichernden Aspekten abgehört würden. Ergänzend verwies der Leiter des Rettungsdienstes darauf, dass das Abhören der Aufzeichnungen durch den ärztlichen Leiter eine Folge von Beschwerden über Fehlentscheidungen sei. Gemäß § 10 Abs. 3 RettDG LSA sei der Ärztliche Leiter zum qualitätssichernden Abhören befugt. Die Überprüfung erfolge anlassbezogen und auf das notwendige Mindestmaß beschränkt. Es läge keine Mitarbeiterüberwachung vor, auch sei keine vorherige Information an die Mitarbeiter geboten.

Der Landesbeauftragte teilte die Auffassung, dass es dem Ärztlichen Leiter zum Zwecke der Überwachung der Tätigkeit der Rettungsdienstleitstelle und zur Qualifikation des Rettungsdienstpersonals gestattet ist, die Dokumentationen nach § 20 RettDG LSA abzuhören, soweit das erforderlich und insgesamt verhältnismäßig ist. Insbesondere ist auch die Überprüfung von Beschwerdefällen als anlassbezogene Einzelfallmaßnahme möglich. Der Landesbeauftragte machte aber deutlich, dass der im Vordergrund stehende Aspekt der Sicherung des öffentlichen Gesundheitssystems den Aspekt des Schutzes der Persönlichkeitssphäre der Beschäftigten nicht verdränge. Es spiele keine Rolle, ob und inwieweit die Absicht besteht, das System auszunutzen. Ausschlaggebend ist die rein objektive Möglichkeit des Abhörens, die zu einem dauerhaften Überwachungsdruck und damit zu einem Eingriff in die Persönlichkeitsrechte der Beschäftigten führt. Ein Mit- oder Abhören ist nur soweit möglich, wie überwiegende Arbeitgeberinteressen dies gebieten, wie z. B. in der Anlernphase, stichprobenartig zur Qualitätssicherung aufgrund der gesetzlichen Vorgaben oder in konkreten Beschwerdefällen. Zur Reduzierung des Überwachungsdrucks ist eine hinreichende Sicherheit geboten, dass unverhältnismäßige Leistungs- oder Verhaltenskontrollen nicht stattfinden. Soweit danach ein Abhören geboten ist, gilt dies für die gesamte Kommunikation der Rettungsleitstelle und damit ggf. auch für einzelne Amtsnummern, soweit diese für Rettungszwecke genutzt werden und dies durch die Rettungsleitstelle veröffentlicht wurde. Die Amtsnummern der Mitarbeiter der Behörden dürfen grundsätzlich nicht abgehört werden.

14.1.2 Patientendaten-Schutz-Gesetz

Im XVI. Tätigkeitsbericht (Nr. 12.1.1) hatte der Landesbeauftragte auf Erörterungs- und Verbesserungsbedarf zum Entwurf eines Patientendaten-Schutz-Gesetzes (PDSG) hingewiesen. Dem gesetzgeberischen Ziel der Stärkung der Patientenrechte zuwider enthielt der Entwurf datenschutzrechtliche Defizite insbesondere in Bezug auf das Zugriffsmanagement hinsichtlich der elektronischen Patientenakte. Zur Wahrung der Datensouveränität der Versicherten ist es unabdingbar, dass die elektronische Patientenakte von Anfang an mit einem feingranularen, d. h. dokumentenbezogenen Zugriffs-

management des Versicherten ausgestattet ist. Nur so sei gewährleistet, dass der Versicherte Einfluss darauf hat, in welche Unterlagen in der über ihn geführten elektronischen Patientenakte Ärzte, Apotheker oder sonstige Leistungserbringer Einsicht nehmen können. Die vorgesehene Steuerungsmöglichkeit bezieht sich aber zunächst nur auf jeweils alle Daten, die vom Versicherten bzw. von den Leistungserbringern eingegeben werden. Diejenigen, die über ein digitales Endgerät verfügen, können erst ab 2022 differenziert zugreifen. Andere müssen sich weiter der Unterstützung der Leistungserbringer bzw. Dritter bedienen. Dieses defizitäre Zugriffsmanagement ist mit den datenschutzrechtlichen Grundsätzen der Erforderlichkeit, der Zweckbindung, der Datenminimierung sowie der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. b, c und f DS-GVO nicht vereinbar. Das bedeutet: die Beachtung nationalen Rechts mit der Umsetzung der Vorgaben des PDSG steht im Konflikt mit den Anforderungen der europaweit verbindlichen Datenschutz-Grundverordnung. Ebenso bestanden Bedenken in technischer Hinsicht hinsichtlich der Authentifizierungsverfahren.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit äußerte frühzeitig und umfassend seine datenschutzrechtlichen Bedenken. Auch der Bundesrat regte u. a. Prüfungen bzw. Änderungen hinsichtlich des feingranularen Zugriffsmanagements an (BR-Drs. 164/20 Beschluss).

Der Landesbeauftragte teilte die Bedenken zur Ausgestaltung der Patientensouveränität und wies das zuständige Ministerium im August 2020 darauf hin. Mit der Entschließung „Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!“ vom 1. September 2020 **(Anlage 4)** wies die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eindringlich auf datenschutzrechtliche Mängel des PDSG hin. Trotz der massiven Bedenken der Datenschutzaufsichtsbehörden trat das PDSG am 15. Oktober 2020 in Kraft.

Daraufhin fand im Oktober 2020 ein Beratungsgespräch zur Umsetzung des PDSG mit der der Aufsicht des Landesbeauftragten unterstehenden Krankenkasse statt. Die datenschutzrechtlichen Bedenken wurden erörtert. Der Landesbeauftragte wird das Vorgehen der Krankenkasse bei der Umsetzung des PDSG aufmerksam beobachten und, falls erforderlich, auf die Einhaltung europarechtlicher Vorgaben hinwirken.

14.1.3 Übermittlung von Gesundheitsdaten von Taxifahrern mit Hilfe von WhatsApp anlässlich von Krankentransporten

Bereits in seinem XII. Tätigkeitsbericht (Nr. 5.10) und im XIII./XIV. Tätigkeitsbericht (Nr. 5.7) hatte der Landesbeauftragte über die Risiken beim Einsatz des Messengerdienstes WhatsApp berichtet. Den Landesbeauftragten erreichen dennoch immer wieder Informationen, dass der Dienst im betrieblichen Alltag von Unternehmen eingesetzt wird.

So wurde z. B. bekannt, dass ein größeres Taxiunternehmen, das auch Krankentransportfahrten durchführt, eine Chatgruppe im Messengerdienst WhatsApp eingerichtet hatte. Es hatte bis zu 32 seiner Beschäftigten angewiesen, diese Gruppe zu nutzen, um Krankentransportscheine, Zuzahlungsbefreiungskarten und Kostenübernahmeschreiben der Kostenträger (vor allem Krankenkassen) zwischen den Fahrern und den in der Zentrale für die Abrechnung zuständigen Beschäftigten auszutauschen. In der Folge haben die Fahrer diese Unterlagen von rund 200 Fahrgästen mit ihren privaten

Handys fotografiert und diese Fotos in die Chatgruppe eingestellt. Als Zweck hat das Unternehmen eine reibungslose Abrechnung mit den Kostenträgern angegeben, da die Fahrer diesbezüglich nicht im Detail geschult gewesen seien.

Indem das Taxiunternehmen bei der Durchführung von Krankentransportfahrten Daten der Fahrgäste aus den Krankentransportscheinen, Zuzahlungsbefreiungskarten und Kostenübernahmeschreiben der Kostenträger erhebt und weiterverarbeitet, z. B. an Dritte übermittelt, verarbeitet es Gesundheitsdaten und damit besondere Kategorien personenbezogener Daten im Sinne von Art. 4 Nr. 15 und Art. 9 DS-GVO. Daher ist in besonderem Maße mittels geeigneter technischer und organisatorischer Maßnahmen nach Art. 25 und 32 DS-GVO sicherzustellen, dass der Zugriff Unbefugter auf personenbezogene Daten ausgeschlossen ist und auch, dass Zugang zu personenbezogenen Daten nur die Beschäftigten erhalten, die dies für ihre Aufgabenerfüllung benötigen. Daten dürfen nur an Dritte übermittelt werden, wenn dafür eine einschlägige Rechtsgrundlage vorliegt.

Die Nutzung des Messengerdienstes WhatsApp im betrieblichen Alltag begegnet aus verschiedenen Gründen erheblichen datenschutzrechtlichen Bedenken (siehe im Detail bereits oben genannte Tätigkeitsberichte). Das datenschutzrechtliche Risiko war im geprüften Fall wegen der Verarbeitung von Gesundheitsdaten besonders hoch und erhöhte sich nochmals, da zu dienstlichen Zwecken auch private Endgeräte genutzt wurden. Dort findet ggf. eine Vermischung mit privaten Daten und privatem Nutzungsverhalten statt. Darüber hinaus besteht die Gefahr, dass Fotos mit personenbezogenen Daten mittels WhatsApp auf Smartphones – je nach Einstellung – unverschlüsselt weiterverarbeitet werden. Oft werden Fotos, Videos und Sprachnachrichten standardmäßig im externen Speicher bzw. in der Galerie des Smartphones abgespeichert. Andere Apps mit Zugriffsrechten auf den externen Speicher bzw. die Galerie könnten so auf diese Daten zugreifen.

Für die regelmäßige Übermittlung der Kontaktdaten aus dem Adressbuch der WhatsApp-Nutzer an WhatsApp weist der Messengerdienst in den Nutzungsbedingungen darauf hin, dass die Nutzer dies im Einklang mit den geltenden Gesetzen tun. Dies würde nach der DS-GVO erfordern, von allen Kontakten (mindestens jedoch von den Nicht-WhatsApp-Nutzern) eine Einwilligung einzuholen.

WhatsApp weist zudem auf seiner Webseite darauf hin, dass die Nutzer schon durch den Download des Messengers den Nutzungsbedingungen und der Datenschutzrichtlinie zustimmen. Ob diese Zustimmung zu den Nutzungsbedingungen und der Datenschutzrichtlinie durch Installation der App die Anforderungen an eine Einwilligung gemäß Art. 7 und Art. 4 Nr. 11 DS-GVO einschließlich der zugehörigen Erwägungsgründe 32, 42 und 43 der DS-GVO erfüllt, ist höchst fraglich und eher zu verneinen. Bei der Verarbeitung von Gesundheitsdaten kommt hinzu, dass es sich nach Art. 9 Abs. 2 lit. a DS-GVO um eine ausdrückliche Einwilligung handeln müsste. Konkludentes, d. h. schlüssiges Handeln reicht hier nicht aus.

Zudem widerspricht es dem Kopplungsverbot aus Art. 7 Abs. 4 DS-GVO, wenn Nutzer des Messenger-Dienstes diesen nur benutzen können, wenn sie in die Verarbeitung personenbezogener Daten einwilligen, die für die Erbringung des Messenger-Dienstes nicht erforderlich sind.

Neben den beschriebenen allgemeinen Risiken hat die Nutzung der WhatsApp-Gruppe in dem geprüften Taxiunternehmen dazu geführt, dass alle Gruppenmitglieder Zugang zu den Gesundheitsdaten aller betroffenen Fahrgäste hatten. Die Daten waren stets für alle Mitglieder der WhatsApp-Gruppe zugänglich, also auch für die 30 Personen, die an den jeweiligen Beförderungs- und Abrechnungsvorgängen der Kollegen nicht beteiligt waren, was für ihre Aufgabenerfüllung nicht erforderlich war. Der Kreis der Personen, die Zugriffsrechte auf die jeweiligen personenbezogenen Daten hatten, war folglich nicht auf das notwendige Maß beschränkt. Das Unternehmen hat somit eine technische und organisatorische Maßnahme ergriffen, die ungeeignet war, den Anforderungen der DS-GVO zu genügen. Dies stellte einen Verstoß gegen Art. 25 und 32 DS-GVO dar.

Nach der aufsichtsbehördlichen Beratung hat das Unternehmen dieses Verfahren unmittelbar eingestellt, die WhatsApp-Gruppe gelöscht und die Beschäftigten aufgefordert, alle Daten im Zusammenhang mit dieser WhatsApp-Gruppe von den Endgeräten zu entfernen. Die aufsichtsbehördliche Kontrolle wurde mit einer Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO abgeschlossen.

14.1.4 Einwilligung in die Verarbeitung von Gesundheitsdaten

Im XV. Tätigkeitsbericht (Nr. 11.1.2) hatte der Landesbeauftragte bereits dargestellt, dass Arztpraxen keine Einwilligung ihrer Patienten einholen müssen, um deren personenbezogene Daten zur Erfüllung des Behandlungsvertrages zu verarbeiten. Sein entsprechendes Informationsblatt hat der Landesbeauftragte zwischenzeitlich aktualisiert.[36] Neu aufgenommen wurden Anwendungsbeispiele in Arztpraxen, für die eine Einwilligung benötigt wird sowie eine Formulierungshilfe für eine Einwilligungserklärung.

Auch für Apotheken gilt, dass Datenverarbeitungen, die erforderlich sind, um den Vertrag der Apotheke mit den Kunden zu erfüllen, insbesondere die Kunden mit verordneten Arzneimitteln und anderen bestellten Produkten zu versorgen, bereits auf gesetzlicher Grundlage erfolgen und keiner Einwilligung bedürfen (Art. 6 Abs. 1 Satz 1 lit. b i. V. m. Art. 9 Abs. 2 lit. h DS-GVO). Gleiches gilt, wenn eine spezialgesetzliche Norm zu einer Datenverarbeitung verpflichtet oder sie erlaubt. Geht die Apotheke mit der Datenverarbeitung allerdings über die reine Vertragserfüllung oder andere gesetzliche Erlaubnisnormen hinaus, z. B. indem sie Gesundheitsdaten zu werblichen Zwecken verarbeitet oder Serviceleistungen wie eine Stammkundenbetreuung erbringt, bedarf es hierfür der ausdrücklichen, freiwilligen, informierten und widerruflichen Einwilligung der betroffenen Person (vgl. Art. 6 Abs. 1 Satz 1 lit. a i. V. m. Art. 9 Abs. 2 lit. a DS-GVO).

Eine Versandapotheke vertrat in diesem Zusammenhang die Auffassung, dass sie im Rahmen ihrer pharmazeutischen Beratungspflicht (vgl. § 20 ApBetrO) oder auch der Pflicht, Arzneimittelmissbrauch entgegenzutreten (vgl. § 17 Abs. 8 ApBetrO), zur Speicherung und Auswertung aller vorherigen Bestellungen der Kunden verpflichtet sei und daher auch für diese Art der Datenverarbeitung keine Einwilligung einholen müsse.

[36] https://lsaurl.de/RGArztpraxis

Auswirkungen hätte dies vor allem für Gastbesteller, denn bei registrierten Kunden würde eine darauf gerichtete Einwilligung bereits eingeholt.

Der Landesbeauftragte hat sich zu der Frage, wie weit in diesem Sinne die Pflichten der Apotheker nach § 17 Abs. 8 und § 20 ApBetrO reichen, mit der Apothekerkammer Sachsen-Anhalt, die ihrerseits auch die Bundesvereinigung Deutscher Apothekerverbände e. V. eingebunden hat, sowie zu der datenschutzrechtlichen Bewertung auch mit den weiteren Datenschutzaufsichtsbehörden in Deutschland ausgetauscht.

Im Ergebnis vertrat der Landesbeauftragte die Rechtsauffassung, dass Bestelldaten, die in einer Versandapotheke anfallen, nach der vollständigen Zahlungsabwicklung zuzüglich einer möglichst kurzen Überliegefrist auf gesetzlicher Grundlage nur noch zum Zweck der Rezeptabrechnung und zur Erfüllung handels- oder steuerrechtlicher Dokumentationspflichten verarbeitet werden dürfen. Bei der Beratung bei künftigen Bestellungen bleibt die Bestellhistorie grundsätzlich unberücksichtigt. Basis für die Beratung des Apothekers sind die Informationen, die sich anlässlich des konkreten Abgabevorgangs ergeben. Dies ist vergleichbar mit einer Abgabe von Arzneimitteln in Präsenzapotheken. Auch wenn die Eindämmung des Arzneimittelmissbrauchs im Allgemeininteresse und im Individualinteresse des Bestellers liegt, kann dies nicht dazu führen, jegliche Bestellhistorien unbegrenzt zu speichern und (ggf. elektronisch) auszuwerten.

Angesichts der Bedeutung der Gesundheitsversorgung und angesichts eines möglicherweise erhöhten Risiko- und Missbrauchspotenzials im Onlinebereich, wo der persönliche Kontakt fehlt, wäre allerdings vorstellbar, dass bei Bestellungen von besonders risikobehafteten Produkten die Überliegefristen z. B. an der üblichen Einnahmedauer ausgerichtet werden könnten. Dies würde allerdings im Einzelfall eine spezifische Betrachtung der bestellten Produkte erfordern.

Unbenommen bliebe die Möglichkeit, alle Kunden, also auch die Gastbesteller, um ihre ausdrückliche, freiwillige und informierte Einwilligung (vgl. Art. 9 Abs. 2 lit. a DS-GVO) für die Auswertung der gesamten Bestellhistorie zu bitten.

14.1.5 Löschung von Gesundheitsdaten

Durch eine Eingabe wurde dem Landesbeauftragten bekannt, dass eine Versandapotheke in ihren Löschroutinen eine generelle 33-jährige Speicherfrist für alle Daten aus Bestellungen von verschreibungspflichtigen Arzneimitteln und aus Retaxierungen vorgesehen hatte. Bei einer Retaxierung verweigert die Krankenkasse der Apotheke die Bezahlung eines Arzneimittels, das die Apotheke zuvor an einen gesetzlich versicherten Patienten abgegeben hat. Die Versandapotheke begründete dies mit einem zivilrechtlichen Haftungsrisiko. Bei gesundheitlichen Spätfolgen aufgrund der Einnahme von Arzneimitteln seien die Vertriebswege im Einzelfall nachzuweisen. Die zivilrechtlichen Verjährungsfristen betrügen 33 Jahre.

Tatsächlich bestehen in bestimmten Fällen für eine Apotheke sehr lange Aufbewahrungspflichten, z. B. sind Daten über Erwerb und Abgabe von Blutzubereitungen, Sera aus menschlichem Blut und Zubereitungen aus anderen Stoffen menschlicher Herkunft sowie gentechnisch hergestellten Plasmaproteinen zur Behandlung von Hämostasestörungen für die Dauer von 30 Jahren zu speichern (§ 22 Abs. 4 i. V. m. § 17 Abs. 6a ApBetrO). Im Übrigen bestehen jedoch weit kürzere Fristen. So beträgt die

allgemeine Dokumentationspflicht in Apotheken mindestens ein Jahr nach Ablauf des Verfalldatums, jedoch nicht weniger als 5 Jahre (vgl. § 22 Abs. 1 ApBetrO). Die handels- bzw. steuerrechtliche Aufbewahrungspflicht für Buchungsbelege beträgt 10 Jahre, für Handels-/Geschäftsbriefe und sonstige für die Besteuerung relevante Unterlagen 6 Jahre (§ 257 Absätze 1 und 4 HGB sowie § 147 Absätze 1 und 3 der AO). Auf der Internetseite der Apothekerkammer Sachsen-Anhalt ist eine Übersicht über die für Apotheken geltenden Aufbewahrungsfristen abrufbar.

Eine darüberhinausgehende Notwendigkeit, Daten aufzubewahren, könnte sich ergeben, wenn mit der Geltendmachung zivilrechtlicher Ansprüche zu rechnen ist (Art. 9 Abs. 2 lit. f DS-GVO). Soweit bei der Verarbeitung bestimmter Daten im Einzelfall zu befürchten ist, dass gegen den Verantwortlichen Schadensersatzansprüche bestehen könnten, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen (§ 199 Abs. 2 BGB), oder im Einzelfall weitere in § 197 Abs. 1 Nrn. 2 bis 6 BGB genannte Ansprüche bestehen könnten, würde die zivilrechtliche Verjährungsfrist für diese Ansprüche 30 Jahre betragen. Höhere Haftungsrisiken können sich in einer Apotheke zum Beispiel ergeben, wenn der Apotheker Arzneimittel selbst herstellt, etwa bei Rezepturarzneimitteln i. S. v. § 1a Abs. 8 ApBetrO oder dem Herstellen und Verblistern von Arzneimitteln (§ 4 Abs. 14 AMG), oder wenn der Apotheker Medikationspläne oder Medikationsanalysen erstellt (vgl. z. B. § 31a SGB V).

Zu der Frage, wie hoch das Haftungsrisiko für Apotheken einzuschätzen ist, hat der Landesbeauftragte die fachliche Einschätzung der Apothekerkammer Sachsen-Anhalt eingeholt. Diese teilte aufgrund eigener Recherchen und einer bundesweiten Abfrage bei anderen Apothekerkammern mit, dass keine Fallgestaltungen bekannt geworden seien, bei denen eine Apotheke noch nach über 10 Jahren haftungsrechtlich in Anspruch genommen wurde. Eine Rechtsverteidigung erscheine dann unwahrscheinlich. Nur in schwierigen Fällen mit einem hohen Haftungsrisiko wäre dies ggf. abweichend zu bewerten. Dies würde allerdings nur begründete Einzelfälle betreffen.

Der Landesbeauftragte vertrat daher weiterhin die Auffassung, dass eine Aufbewahrungsfrist von 10 Jahren im Regelfall ausreichen sollte und lediglich in begründeten Einzelfällen davon abgewichen werden könnte. Voraussetzung für eine entsprechend längere Aufbewahrung ist, dass nachweislich konkrete Anhaltspunkte dafür bestehen, dass im Einzelfall oder ggf. bei zu bestimmenden Kategorien von Fällen mit der Geltendmachung zivilrechtlicher Ansprüche noch nach mehr als 10 Jahren zu rechnen ist. Eine rein theoretische Möglichkeit einer Geltendmachung vermag die Erforderlichkeit und damit Zulässigkeit weiterer Speicherung nicht zu begründen, vgl. bereits XVI. Tätigkeitsbericht (Nr. 6.12) sowie XI. Tätigkeitsbericht (Nr. 10.1.9). In einer Apotheke ist daher eine differenzierte Betrachtung anhand der Art der abgegebenen Arzneimittel bzw. erbrachten Apothekenleistung sowie dem individuellen Haftungsrisiko und eine entsprechend differenzierte Umsetzung der Löschzyklen erforderlich.

Seine Auffassung hatte der Landesbeauftragte bereits in einem Informationsblatt im September 2015 veröffentlicht. Das Informationsblatt „Datenschutzgerechte Vernichtung von Gesundheitsdaten“ steht seit Oktober 2020 in einer aktualisierten Fassung[37] bereit. Es richtet sich an alle medizinischen Einrichtungen und Verantwortlichen, deren

[37] https://lsaurl.de/GesDatVern

Geschäftstätigkeit notwendigerweise mit der Verarbeitung von Gesundheitsdaten verbunden ist. Es berücksichtigt sowohl die Einführung der DS-GVO, die Neufassung des BDSG und das DSAG LSA als auch die Ergänzung des § 203 StGB im Hinblick auf die „mitwirkenden Personen“, vgl. XIII./XIV. Tätigkeitsbericht (Nr. 10.1.8). Es enthält Ausführungen zu den rechtlichen Grundlagen, zu Umfang, Zeitpunkt sowie Art und Weise der Vernichtung.

Gleichzeitig hat der Landesbeauftragte auch eine Formulierungshilfe für einen Auftragsverarbeitungsvertrag für die Vernichtung von Gesundheitsdaten[38] bereitgestellt. Diese Formulierungshilfe kann Auftraggebern und Auftragnehmern eine Grundlage für einen eigenen Vertragsentwurf oder für die Prüfung bereits vorhandener Verträge sein.

14.2 Sozialwesen

14.2.1 Kopieren des Personalausweises

Der Landesbeauftragte äußerte bereits in seinem VII. Tätigkeitsbericht (Nr. 20.4) Kritik an der Praxis von Sozialleistungsträgern, regelmäßig den Personalausweis von Antragstellern für die Akte zu kopieren. Mit seinem XI. Tätigkeitsbericht (Nr. 10.2.2) gab der Landesbeauftragte Hinweise, unter welchen engen Voraussetzungen die Aufnahme einer Kopie des Personalausweises in die Akte eines Jobcenters aus datenschutzrechtlicher Sicht zulässig wäre. So ist denkbar, dass die Kopie auf der Grundlage einer informierten und freiwilligen Einwilligung gespeichert werden darf, damit sich Antragsteller nicht bei jeder Vorsprache mit ihrem Personalausweis erneut identifizieren müssen.

Im Berichtszeitraum kam es zu einer Beschwerde, weil ein Jobcenter – unter Hinweis auf bestehende Mitwirkungspflichten und unter Androhung der Leistungsversagung – mehrfach eine Einverständniserklärung zum Kopieren und Aufbewahren von Ausweisdokumenten anforderte. Genau dieses Jobcenter wurde bereits zwei Jahre zuvor zu dem Erfordernis einer informierten und freiwilligen Einwilligungserklärung beraten. Es hatte zugesichert, die Einwilligungserklärung zu überarbeiten und die Beschäftigten zu sensibilisieren, dass in diesem Zusammenhang weder Mitwirkungspflichten bestehen noch Sanktionen drohen. Durch die Beschwerde war es erneut erforderlich, das Jobcenter zu den Voraussetzungen zu beraten. So darf nur dann eine Kopie des Personalausweises zur Akte genommen werden, wenn der Antragsteller einwilligt. Diese Einwilligung ist nur wirksam, wenn sie auf einer freiwilligen Entscheidung des Betroffenen beruht. Freiwilligkeit bedeutet, dass eine echte Wahl besteht, das Einverständnis zu erteilen oder nicht zu erteilen. Enthält jedoch das Formular zur Einwilligungserklärung gar keine Möglichkeit, sich gegen das Kopieren zu entscheiden oder wird es verbunden mit einer Fristsetzung zur Rückgabe und Hinweisen auf Mitwirkungspflichten nach §§ 60 ff. SGB I, kann von einer auf dem freien Willen beruhenden Einverständniserklärung nicht ausgegangen werden. Das Jobcenter wurde erneut beraten und wird künftig darauf achten, dass die Einwilligung datenschutzkonform eingeholt wird.

14.2.2 Meldungen von Datenschutzverletzungen

Die Zahl der beim Landesbeauftragten eingegangenen Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO im Bereich des

[38] https://lsaurl.de/AVVGesDatVern

Sozialwesens bewegt sich auf dem Niveau des letzten Berichtszeitraums, vgl. XVI. Tätigkeitsbericht (Nr. 12.2.1). Wiederum bildete der Fehlversand einzelner Anlagen oder ganzer Schreiben einen Schwerpunkt der eingegangenen Meldungen. Zum Vorgehen in diesen Fällen weist der Landesbeauftragte darauf hin, dass zur Abmilderung der Auswirkungen ein besonderes Augenmerk auf die Auswahl der zu ergreifenden Maßnahmen gelegt werden sollte. Wenn der versehentliche Empfänger gebeten wird, das fehlversandte Schreiben zurückzusenden, sollte dem Schreiben zur Erhöhung der Bereitschaft ein Freiumschlag beigefügt werden. Dies ermöglicht der Behörde die datenschutzgerechte weitere Aufbewahrung oder Vernichtung der Daten und verhindert, dass das Schreiben beim versehentlichen Empfänger ggf. im Hausmüll oder in der Papiertonne entsorgt wird, was ein starkes Missbrauchspotential durch weitere Personen birgt. Der Empfänger sollte zusätzlich aufgefordert werden, Verschwiegenheit über die ihm unrechtmäßig bekannt gewordenen Daten zu bewahren, und er sollte gebeten werden, zu versichern, dass er die Daten vollständig zurückgegeben, also insbesondere keine Kopien gefertigt hat.

14.2.3 Aufbewahrung von Leistungsakten

Wurden Sozialdaten zunächst in zulässiger Weise verarbeitet, dürfen Sozialleistungsträger sie dennoch nicht unbegrenzt aufbewahren. Sind die Daten für die Zwecke, für die sie erhoben und verarbeitet wurden, nicht mehr notwendig, ist der für die Verarbeitung Verantwortliche verpflichtet, diese Daten unverzüglich zu löschen (Art. 17 Abs. 1 lit. a DS-GVO). Eine Ausnahme dazu nennt § 84 Abs. 1 Satz 1 SGB X für Fälle der besonderen Art der Speicherung bzw. des unverhältnismäßig hohen Löschungsaufwands. Es stellt sich häufig die Frage, ab wann die Daten nicht mehr notwendig sind.

Eine im Berichtszeitraum eingegangene Beschwerde richtete sich gegen ein Sozialamt einer kreisfreien Stadt. Dieses weigerte sich, die personenbezogenen Daten des mit Einführung des Angehörigen-Entlastungsgesetzes seit dem 1. Januar 2020 nicht mehr unterhaltspflichtigen Angehörigen einer Pflegebedürftigen unverzüglich zu löschen. Das um Stellungnahme gebetene Sozialamt teilte mit, dass weiterhin Leistungen an die pflegebedürftige Person geleistet werden und eine Löschung der Sozialhilfeakte erst nach Ablauf der Aufbewahrungsfristen, die erst nach Beendigung der Leistung zu laufen beginne, erfolgen werde. Im Übrigen, so meinte das Sozialamt, lege die Aktenordnung des Landes Sachsen-Anhalt für Hauptakten eine zwanzigjährige Aufbewahrungsfrist fest.

Dass Verwaltungsvorgänge auch nach ihrem Abschluss für eine gewisse Zeit aufbewahrt werden, ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Zu den typischen Verwaltungsabläufen gehören auch nach der Beendigung von Leistungen andere Verwaltungsvorgänge, wie beispielsweise nachträgliche Prüfungen durch Rechnungsprüfungsbehörden oder die Überprüfung gewährter Leistungen nach Vorliegen neuer Erkenntnisse. Dazu werden Verwaltungsvorgänge auch nach der Einstellung von Sozialleistungen für einen begrenzten Zeitraum aufbewahrt. Das Sozialamt ging jedoch fehl in der Annahme, dass es sich bei Sozialhilfeakten um Hauptakten handelt. Hauptakten sind Akten, die Dokumente von allgemeiner oder grundsätzlicher, genereller Bedeutung enthalten. Dies können Gesetze, Verordnungen, Satzungen, Bekanntmachungen, Erlasse oder Verfügungen allgemeinen Charakters sowie Entscheidungen von grundsätzlicher Bedeutung sein. Nebenakten fassen hingegen Dokumente von begrenzter, spezieller Bedeutung zusammen, die einzelne Personen, Sa-

chen, Ereignisse oder Rechtsverhältnisse wie Genehmigungen oder Erlaubnisse betreffen. Leistungsakten der Sozialleistungsträger betreffen grundsätzlich einzelne Personen oder kleine Personengruppen, z. B. Familien oder Lebens- bzw. Haushaltsgemeinschaften. In ihnen werden Regelungen zu Einzelfällen festgehalten, jedoch keine Regelungen über den Einzelfall hinaus dokumentiert. Es dürfte sich bei den in der Leistungsverwaltung typischen Einzelfallakten demnach um Nebenakten handeln, für die üblicherweise eine sehr viel kürzere Aufbewahrungsfrist gilt (maximal 5 Jahre). Im Interesse der beschleunigten Aussonderung des für die praktische Verwaltungsarbeit nicht mehr benötigten Schriftguts soll die Aufbewahrungsdauer nach § 18 Abs. 1 lit. a AktO möglichst kurz bemessen werden, vgl. zu weiteren Aspekten der Aufbewahrung und Löschung auch den Beitrag „Löschungspflicht und Verjährungsfrist“ im XVI. Tätigkeitsbericht (Nr. 6.12) und den Beitrag „Langfristige Aufbewahrung von Patientenakten“ im XI. Tätigkeitsbericht (Nr. 10.1.9).

14.2.4 Anforderung und Aufbewahrung von Kontoauszügen durch Jobcenter

Im Bereich des Sozialwesens bleibt die Frage der Zulässigkeit von Anforderung und Speicherung von Kontoauszügen ein Dauerthema. Bereits im XII. Tätigkeitsbericht (Nr. 11.2.1) und im XV. Tätigkeitsbericht (Nr. 11.2) hat der Landesbeauftragte dazu umfassend informiert. Nun haben sich weitere Entwicklungen ergeben:

In seinem Urteil vom 14. Mai 2020 hat sich das Bundessozialgericht (Az: B 14 AS 7/19 R, juris) mit dem Antrag einer Klägerin auf Löschung ihrer Kontoauszüge befasst. Diese wollte erreichen, dass nach der Einstellung der Leistungen ihre Kontoauszüge aus ihrer Leistungsakte entfernt werden. Das Jobcenter lehnte dies jedoch für Kontoauszüge ab, sofern diese Angaben enthielten, die die Höhe des Leistungsbezuges beeinflussen. Das Bundessozialgericht stellte jedoch fest, dass Kontoauszüge mit Angaben zu Zahlungseingängen für einen Zeitraum von zehn Jahren nach Bekanntgabe der Leistungsbewilligung gespeichert werden dürfen. Solange nachträgliche Änderungen der Bewilligungsentscheidungen nicht ausgeschlossen sind, muss das Jobcenter Zugriff auf die bei Antragstellung vorgelegten Informationen haben. Der damit verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung ist verfassungsrechtlich gerechtfertigt. Voraussetzung bleibt aber, dass nicht leistungsrelevante Angaben über Zahlungsempfänger auf Kontoauszügen geschwärzt werden können und die Einsicht in die Kontoauszüge auf zulässige Zwecke beschränkt bleibt, was das Jobcenter sicherzustellen hat.

Im Berichtszeitraum forderten Jobcenter Kontoauszüge nicht mehr für die letzten drei, sondern für sechs Monate an. Dies begründeten sie damit, dass der Bewilligungszeitraum statt sechs nun zwölf Monate betrage. Auch die „Fachliche Weisung der Bundesagentur für Arbeit zum Zweiten Sozialgesetzbuch“ sehe das so vor. Der entgegenstehenden Auffassung der Datenschutzaufsichtsbehörden des Bundes und der Länder, dass es für die Prüfung des Leistungsanspruchs auch bei einem Bewilligungszeitraum von zwölf Monaten ausreicht, die Kontoauszüge der letzten drei Monate vorzulegen, hat sich die Bundesagentur für Arbeit inzwischen angeschlossen.

Für die Prüfung des Leistungsanspruchs ist auch bei einem Bewilligungszeitraum von 12 Monaten die Vorlage der Kontoauszüge der letzten drei Monate grundsätzlich ausreichend.

Grundsätzlich dürfen auch weiterhin Daten nur so lange gespeichert werden, wie diese zur rechtmäßigen Erfüllung der Aufgaben des Sozialleistungsträgers erforderlich sind. Kontoauszüge, die Angaben zu Zahlungseingängen enthalten, können für einen Zeitraum von zehn Jahren nach Bekanntgabe der Leistungsbewilligung erforderlich sein und deshalb für diesen Zeitraum gespeichert werden.

15 Statistik, Kommunales

15.1 Zensus 2021 – Verschiebung auf 2022

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

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

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

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

15.2 Behördliche Datenschutzbeauftragte der Kommunen

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

Vor diesem Hintergrund hat der Landesbeauftragte alle Kommunen im Land Sachsen-Anhalt schriftlich um Mitteilung der Kontaktdaten des jeweiligen Datenschutzbeauftragten gebeten. Diese Gelegenheit hat der Landesbeauftragte auch dazu genutzt,

durch Mitteilung der direkten Kontaktdaten der Ansprechpartner für kommunale Fragen in seinem Haus zur Verbesserung der Kommunikation zwischen den Datenschutzbeauftragten der Kommunen und ihm beizutragen. Über diesen direkten Weg zu den Datenschutzbeauftragten der Kommunen beabsichtigt der Landesbeauftragte künftig wichtige Informationen den Datenschutzbeauftragten der Kommunen direkt zu übermitteln.

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

15.3 Kommunales Online-Portal „Sag's uns einfach"

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

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

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

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

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

15.4 Kommunalverfassungsgesetz

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

Dieser Problematik sollte der Entwurf eines „Zweiten Gesetzes zur Änderung des Kommunalverfassungsgesetzes" dadurch Rechnung tragen, dass Regelungen zu „Verfahren in außergewöhnlichen Notsituationen" geschaffen werden. Zum einen sollte die Durchführung von Sitzungen der Vertretung und ihrer Ausschüsse mittels

Videokonferenztechnik ermöglicht werden, zum anderen sollten die Vertretung und ihre Ausschüsse über Verhandlungsgegenstände im Wege eines schriftlichen oder elektronischen Verfahrens abstimmen können.

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

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

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

15.5 Erteilung von Personenstandsurkunden

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

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

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

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

15.6 Hundebestandsaufnahme zur Erfassung steuerpflichtiger Hundehalter

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

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

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

Die Gemeinde wurde darauf hingewiesen, dass ein Verfahren zur Bestandsaufnahme, bei welchem durch die Feststellung des Vorhandenseins einer Besteuerungsgrundlage steuerrelevante Daten erhoben werden, bereits dem Steuerverwaltungsverfahren zuzurechnen ist. Steuerverwaltungsverfahren sind Teil der Eingriffsverwaltung und können bereits deswegen nicht wirksam einwilligungsbasiert ausgestaltet werden. Das Über- und Unterordnungsverhältnis zwischen Staat und Bürgern steht hierbei bereits konzeptionell der datenschutzrechtlich geforderten Freiwilligkeit einer Einwilligung entgegen.

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

16 Wirtschaft

16.1 Meldungen von Datenschutzverletzungen

Wie bereits im letzten Berichtszeitraum kam es auch im Kalenderjahr 2020 zu einer Fülle von Meldungen von Datenschutzverletzungen. Dies ist insoweit ein gutes Zeichen, als die Meldepflicht in der Wirtschaft bekannt geworden ist und erfüllt wird. Allerdings wurden dem Landesbeauftragten z. B. durch Beschwerden betroffener Personen Vorgänge bekannt, die meldepflichtig waren, aber nicht oder mit erheblicher zeitlicher Verzögerung gemeldet wurden.

Meldefrist

Die Überschreitung der Meldefrist beruhte teilweise auf fehlerhaften Rechtsauffassungen und teilweise auf organisatorischen Mängeln.

Im Falle einer Datenschutzverletzung muss die Meldung durch den Verantwortlichen unverzüglich und möglichst binnen 72 Stunden erfolgen, nachdem die Verletzung bekannt wurde (Art. 33 Abs. 1 DS-GVO). Ein Verantwortlicher vertrat die Auffassung, die Meldefrist beginne erst dann zu laufen, wenn der Unternehmensleiter persönlich Kenntnis von der Datenschutzverletzung erlange. Darauf kommt es jedoch nicht an. Die Frist zur Meldung einer Datenschutzverletzung beginnt, wenn der Verantwortliche von dem meldepflichtigen Ereignis Kenntnis erlangt hat. Verantwortlicher ist nach Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies ist das Unternehmen als Ganzes, nicht allein der Leiter. Die

Kenntnisnahme der Mitarbeiter, die entsprechend zu schulen sind, sind dem Unternehmen damit zuzurechnen. Das gilt jedenfalls dann, wenn Mitarbeiter auftragsgemäß den Verdacht einer Datenpanne zu prüfen und gegebenenfalls weiterzuleiten haben. Rein persönliche Hinderungsgründe des Leiters des Unternehmens, wie z. B. Urlaub, wirken grundsätzlich nicht fristverlängernd. Hier sind Vertretungsmaßnahmen zu ergreifen. Ob der Verantwortliche die ihm bekannten Tatsachen rechtlich fehlerhaft nicht als Verletzung i. S. d. Art. 4 Nr. 12 DS-GVO wertet, ist ebenso nicht von Belang.

In organisatorischer Hinsicht sollte durch unternehmensinterne Festlegungen sichergestellt werden, dass die Meldung fristgerecht ergehen kann. Es ist nicht erforderlich, dass nur eine bestimmte Person die Meldung absetzt, z. B. der betriebliche Datenschutzbeauftragte (dessen Aufgabe es ohnehin nicht wäre, vgl. Art. 39 DS-GVO). Es muss stets ein Mitarbeiter in der Lage sein, eine fristgerechte Mitteilung an den Landesbeauftragten zu senden.

Inhalte der Meldungen

Auch in 2020 kam es erneut zu zahlreichen Meldungen, die das Abhandenkommen von Datenträgern oder Fehlzustellungen von Briefpost oder E-Mails zum Inhalt hatten. Insoweit wird zunächst auf die Ausführungen zu Nr. 14.2 des XVI. Tätigkeitsberichts verwiesen.

Zu Fehlversendungen kam es auch aufgrund von Namens- oder Adressänderungen. Verantwortliche sind daher gehalten, eine ständige Aktualisierung von Namen und Kontaktdaten zu gewährleisten, siehe zu Empfehlungen bei Fehlversendungen auch Nr. 13.2.2.

Einen besonders drastischen Verstoß gegen den Datenschutz beging eine Pflegekraft, die Fotografien von teilweise unbekleideten Bewohnern mit ihrem privaten Handy angefertigt und anschließend an ihren ehemaligen Lebensgefährten versandte. Die Tat wurde mit einem empfindlichen Bußgeld geahndet.

Mehrfach kam es zu Fehlversendungen unter Nutzung von Telefaxgeräten. Das Versenden vertraulicher Informationen als Telefax ist nicht ohne Risiko. Informationen können durch eine fehlerhafte Anwahl bei einem falschen Empfänger oder beim richtigen Empfänger in die Hände von Unbefugten geraten. Die Informationen werden grundsätzlich offen (unverschlüsselt) übertragen. Eine Telefaxübersendung kann deshalb mit dem Versand einer offenen Postkarte verglichen werden. Der Telefaxverkehr ist wie ein Telefongespräch abhörbar. Zudem können Rufumleitungen dazu führen, dass Telefaxgeräte zeitweise auf andere Anschlüsse geschaltet sind. Der Landesbeauftragte rät daher dringend davon ab, personenbezogene Daten, deren Offenbarung ein normales bis hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen – dies betrifft regelmäßig besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO wie z. B. Gesundheitsdaten oder die Gewerkschaftszugehörigkeit – per Fax zu übertragen. In den übrigen Fällen, bei denen ein Fax zum Einsatz kommen kann, sind insbesondere mit den Empfängern die Sendezeitpunkte und die Empfangsgeräte abzustimmen, damit das Fax direkt entgegengenommen werden kann und vor der Einsichtnahme Dritter geschützt ist. Die Absprachen schützen auch vor Fehlleitungen,

beispielsweise aufgrund veralteter Anschlussnummern oder aktivierter Anrufumleitungen bzw. -weiterleitungen. Die vom Empfangsgerät vor der Übertragung abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Verbindung unverzüglich abgebrochen werden kann. Sende- und Empfangsprotokolle sind vertraulich abzulegen, da auch sie dem Fernmeldegeheimnis unterliegen.

Alle von den Telefaxgeräten angebotenen Sicherheitsmaßnahmen (beispielsweise Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Passwort, Sperrung der Fernwartungsmöglichkeit) sollten genutzt werden. Die eingestellten technischen Parameter und Speicherinhalte sind regelmäßig, insbesondere nach durchgeführten Wartungen, zu überprüfen. Damit können Fehleinstellungen oder Manipulationsversuche frühzeitig erkannt und verhindert werden. Sofern nicht geschehen sollte der Faxversand – wie auch die gesamte Nutzung von Telefaxgeräten – durch eine Dienstanweisung geregelt werden.

Das Versenden von Faxen ist im Fall einer nichtexistierenden durchgehenden Verschlüsselung und aufgrund der Nichtvorhersagbarkeit derselben als unsicher anzusehen. Hier wäre die Nutzung einer flächendeckenden Transportverschlüsselung – analog der E-Mail-Technologie (vgl. Nr. 6.10) – etwa via SIPS/TLS (SIP Secure und Transport Layer Security; SIP über TLS) und SRTP (Secure Real-Time Transport Protocol) zu fordern.

In etlichen Fällen wurde gemeldet, dass die Informationstechnik vom Emotet-Virus befallen war. Dieses Virus versendet unter Nutzung des Adressverzeichnisses des E-Mailprogramms des befallenen Rechners eigenständig E-Mails. Der Landesbeauftragte verwies in diesen Fällen im Wesentlichen auf die Homepage des Bundesamtes für Sicherheit in der Informationstechnik,[39] in der Abwehrmaßnahmen beschrieben sind. Ähnlich verhielt es sich bei Meldungen eines Befalls mit Ransomware. Auch ohne anschließende Erpressung monetärer Güter und ohne Abfluss von Daten kann eine Verschlüsselung der gesamten Speicherinhalte die Verfügbarkeit einer Datenverarbeitung empfindlich beeinträchtigen. Tägliche Datensicherungen können dem entgegenwirken. Auch hier verwies der Landesbeauftragte regelmäßig auf die Informationsschrift des Bundesamtes für Sicherheit in der Informationstechnik zu Ransomware.[40] In vielen gemeldeten Fällen von Virenbefall verwies der Landesbeauftragte darauf, dass befallene Systeme neu aufzusetzen sind, da Viren sonst nicht mit absoluter Gewissheit vollständig beseitigt werden können und Überreste oder bereits nachgeladene weitere Schadprogramme im System verbleiben und erst nach einiger Zeit wieder aktiv werden könnten.

Im Bereich der Kreditinstitute haben Beschäftigte mehrfach Kontodaten von ihren Verwandten oder Bekannten zu privaten Zwecken abgerufen und genutzt. Dieses Verhalten führt regelmäßig zur Einleitung von verwaltungsrechtlichen oder bußgeldrechtlichen Verfahren gegen die Beschäftigten, da diese im Falle der Verarbeitung zu nicht dienstlichen Zwecken selbst verantwortlich sind (sog. Mitarbeiterexzess). Hier müssen aber auch die Kreditinstitute alles unternehmen, um durch technische und organisatorische Maßnahmen unberechtigte Kontenzugriffe so weit wie möglich zu verhindern. Der Landesbeauftragte hält die Implementierung von Rollenkonzepten für erforderlich,

---

[39] https://lsaurl.de/bsiemotet

[40] https://lsaurl.de/bsiransomware

die den Kontenzugriff der Beschäftigten auf das für ihre Fachaufgabe absolut erforderliche Maß beschränken. Zudem sollten lesende Zugriffe der Beschäftigten protokolliert und angemessen, z. B. durch den Datenschutzbeauftragten, kontrolliert werden.

Pflicht zur Benachrichtigung der betroffenen Personen

Häufig erinnerte der Landesbeauftragte daran, dass die betroffenen Personen nach Art. 34 DS-GVO zu benachrichtigen sind, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat. Ob ein hohes Risiko vorliegt, hängt im Wesentlichen von der Eintrittswahrscheinlichkeit und der Schwere eines möglichen Schadens ab. Wobei das Gesamtrisiko das Produkt von Eintrittswahrscheinlichkeit und Schadensschwere darstellt, und somit durch beide Faktoren gleichermaßen erhöht wird. Umgekehrt unterliegt eine Verarbeitung, bei der die Eintrittswahrscheinlichkeit für einen Schaden gering ist, auch dann einem hohen Risiko, wenn die Schwere des potentiellen Schadens entsprechend hoch ist. Sind besondere Kategorien personenbezogener Daten oder auch Kontodaten von der Datenschutzverletzung betroffen, liegt ein hoher Schaden sehr nahe, insbesondere dann, wenn diese Daten bereits unberechtigt oder unbefugt offengelegt worden sind. In diesen Fällen wären die betroffenen Personen zu benachrichtigen. Der Landesbeauftragte wies mehrfach auf diese Umstände hin, woraufhin es mehrfach zur nachträglichen Benachrichtigung betroffener Personen kam. Es ist Aufgabe des Verantwortlichen, im Einzelfall zu ermitteln, ob ein hohes Risiko vorliegt. Der Landesbeauftragte rät, die Benachrichtigung der betroffenen Personen schon dann vorzunehmen, wenn dies zu einer Risikominimierung beiträgt.

16.2 Änderung des Genossenschaftsrechts

Anlässlich einer Beschwerde hat der Landesbeauftragte die Verbände der Wohnungswirtschaft in Sachsen-Anhalt auf seine rechtliche Bewertung hinsichtlich § 43a Abs. 6 GenG aufmerksam gemacht.

Diese Vorschrift betrifft die Bekanntmachung der Namen und Kontaktdaten der Vertreter und Ersatzvertreter in der Vertreterversammlung einer Genossenschaft. Seit der Änderung dieser Vorschrift zum 22. Juli 2017 sind nicht nur die Namen und Anschriften, sondern nunmehr Namen und zusätzlich wahlweise Anschriften, Telefonnummern oder E-Mail-Adressen bekanntzumachen. Die Bekanntmachung kann wie bisher durch Auslegen in den Geschäftsräumen der Genossenschaft und ihren Niederlassungen geschehen (Frist: mindestens zwei Wochen), aber nun alternativ auch durch Veröffentlichung auf der Internetseite der Genossenschaft (Frist: bis zum Ende der Amtszeit der Vertreter).

Auch hier ist der Grundsatz der Datenminimierung zu beachten (Art. 5 Abs. 1 lit. c DS-GVO). Dies kommt bereits in der Begründung des Gesetzgebers zur Änderung des § 43a GenG zum Ausdruck (vgl. BT-Drs. 18/11506, S. 29). Daraus ergibt sich Folgendes:

In der Regel entscheidet das jeweilige Mitglied der Vertreterversammlung selbst, welche seiner Kontaktdaten auf der Liste ausgewiesen werden (Anschrift, Telefonnummer, E-Mail-Adresse).

Wenn sich die Genossenschaft für die Veröffentlichung im Internet entscheidet, sollte dies in einem nur für die Mitglieder der Genossenschaft zugänglichen Bereich der Internetseite erfolgen. Denn Zweck der Regelung ist, dass die Mitglieder die gewählten Vertreter erreichen können. Es ist damit nicht erforderlich, diese personenbezogenen Daten über einen sehr langen Zeitraum (die gesamte Amtszeit) weltweit allen Besuchern der Internetseite, und damit einem unbestimmten Personenkreis, offenzulegen.

Ebenfalls zum 22. Juli 2017 wurde § 30 GenG geändert, der den Inhalt und das Führen der Mitgliederliste der Genossenschaft regelt. Wie bisher hat der Vorstand in der Mitgliederliste für jedes Mitglied der Genossenschaft den vollständigen Namen, die Anschrift, die Zahl der weiteren Geschäftsanteile sowie das Ausscheiden aus der Genossenschaft einzutragen. Neu ist, dass die Genossenschaft in ihrer Satzung regeln kann, mit welchen weiteren Angaben jedes Mitglied eingetragen wird. Die Gesetzesbegründung benennt als Beispiele die Unternehmereigenschaft, die Eigenschaft als investierendes Mitglied, den Beruf (vgl. BT-Drs. 18/11506, S. 27). Die Genossenschaften müssen allerdings darauf achten, dass nur die weiteren Angaben satzungsmäßig verlangt werden, die wirklich erforderlich sind.

Bisher waren zu jeder eingetragenen Angabe der Zeitpunkt, zu dem sie wirksam wurde, sowie die die Eintragung begründenden Tatsachen anzugeben. Nunmehr ist (nur noch) der Zeitpunkt, zu dem der Beitritt, eine Veränderung der Zahl weiterer Geschäftsanteile oder das Ausscheiden wirksam wird oder geworden ist, anzugeben. Ob es erforderlich ist, dass in der Mitgliederliste (weiterhin) auch für weitere Eintragungen der Änderungszeitpunkt und die die Eintragung begründenden Tatsachen dokumentiert werden (z. B. Namensänderung aufgrund von Eheschließung am …), wäre im Detail zu prüfen und bei Bedarf in der Satzung zu regeln.

Des Weiteren führt die Gesetzesänderung dazu, dass die oft jahrzehntelange Aufbewahrungsfrist von drei Jahren nach Ende des Kalenderjahres, in dem das Mitglied aus der Genossenschaft ausgeschieden ist, nur noch für eintragungsbegründende Unterlagen gilt, die den Beitritt, der Veränderung der Zahl weiterer Geschäftsanteile oder das Ausscheiden betrifft. Für Unterlagen, die sonstige Eintragungen betreffen, gelten die Regelungen für Handelsbriefe in § 257 HGB; sie sind somit derzeit für die Dauer von sechs Jahren nach dem Ende des Eintragungsjahrs aufzubewahren.

16.3 Kontrolle eines Wohnungsunternehmens aufgrund anonymer Mitteilung

Der Landesbeauftragte erhielt einen anonymen Hinweis auf möglicherweise rechtswidrige Datenverarbeitungen bei einem Vermieter, der weit über eintausend Wohneinheiten vermietet. Die Hinweise bezogen sich auf die Speicherung von Personalausweiskopien und Bonitätsdaten von Mietinteressenten und darauf, dass deren Daten in Papierform und elektronisch über viele Jahre hinweg gespeichert würden. Die Vermietungsprozesse seien längst abgeschlossen gewesen und die Daten würden nicht mehr benötigt. Die Hinweise waren sehr detailliert, konkret und glaubhaft. Dazu schilderte der Hinweisgeber, dass der Geschäftsleitung des Unternehmens bewusst gewesen sei, dass es sich um Datenschutzverstöße handeln dürfte und dass vor einer angekündigten Prüfung der Datenschutzaufsichtsbehörde sehr wahrscheinlich Beweise vernichtet werden würden.

Nach eingehender Prüfung entschied sich der Landesbeauftragte unter Würdigung der Umstände dieses Einzelfalles für eine unangekündigte Prüfung in den Geschäftsräumen des Unternehmens. Hierzu ist er nach Art. 58 Abs. 1 lit. f und e DS-GVO i. V. m. § 40 Abs. 5 BDSG berechtigt. Da auch Vorwürfe im Raum standen, die Bußgeldtatbestände berührten, hat der Landesbeauftragte gleichzeitig ein Bußgeldverfahren eröffnet und für den Fall, dass dies notwendig werden sollte, einen Durchsuchungsbeschluss des Amtsgerichts beantragt, der auch ausgestellt wurde.

Die Kontrolle vor Ort bestätigte weitgehend den vom Hinweisgeber vorgetragenen Sachverhalt. Das Unternehmen hatte Daten von Mietinteressenten in einem für den Vermietungsprozess nicht notwendigen Ausmaß erhoben, z. B. sehr persönliche Daten über Familien- und Verwandtschaftsverhältnisse, die persönliche Lebenssituation (Bemerkungen wie „Trennung“, „schwanger“ und „rausgeflogen“ sowie zu familiären Problemen, Erkrankungen, Alkoholproblemen von Angehörigen und häuslicher Gewalt), den Grund des Umzugs, aber auch Kopien von Personalausweisen und Aufenthaltstiteln, bedenkliche Vorvermieterbescheinigungen sowie zusätzlich Bonitätsauskünfte einer Auskunftei. Hinzu kam, dass das Unternehmen die Daten und Unterlagen von Mietinteressenten, bei denen es nicht zu einem Vertragsabschluss gekommen ist, tatsächlich über einen sehr langen Zeitraum aufbewahrte. Die Beschäftigten des Landesbeauftragten fanden in den Geschäftsräumen viele Aktenordner und in der Datenhaltung des Unternehmens Excel-Tabellen mit Mietinteressentendaten, deren Erhebung bis ins Jahr 2013 zurückreichte. Die Vermietungsprozesse waren längst abgeschlossen; es war nicht ersichtlich, warum es erforderlich sein könnte, die Unterlagen und Daten über diese Dauer aufzubewahren. Die Daten hätten daher schon längst gelöscht sein müssen (Art. 17 Abs. 1 lit. a DS-GVO; siehe auch bereits XIII./XIV. Tätigkeitsbericht, Nr. 13.10).

Der Landesbeauftragte klärte über die rechtlichen Grundlagen und den rechtlich zulässigen Umfang der Datenerhebung auf (vgl. Orientierungshilfe der Datenschutzkonferenz zur „Einholung von Selbstauskünften bei Mietinteressentinnen“[41]). Nach der Prüfung vor Ort hatte das Unternehmen Gelegenheit, zu dem vorgefundenen Sachverhalt Stellung zu nehmen. Es fand eine Nachprüfung in den Geschäftsräumen des Unternehmens einschließlich eines ausführlichen Beratungsgesprächs statt. In dem anschließenden Schriftwechsel sicherte das Unternehmen die künftige Beachtung der datenschutzrechtlichen Vorgaben zu. Im Ergebnis hat es seine Formulare und das Löschkonzept angepasst sowie interne Regelungen in Form eines Datenschutzhandbuches eingeführt.

Für die massiven Datenschutzverstöße verhängte der Landesbeauftragte Geldbußen nach § 43 Abs. 3 BDSG a. F. und nach Art. 58 Abs. 2 lit. i DS-GVO, Art. 83 Abs. 5 DS-GVO. Gegen die Bußgeldbescheide legte das Unternehmen Einspruch ein. In der Hauptverhandlung Anfang 2021 stellte das Amtsgericht Magdeburg u. a. das Verfahren bezüglich der Verstöße nach BDSG a. F. ein. Im Übrigen nahm das Unternehmen den Einspruch zurück. Die Geldbußen wurden in Höhe von insgesamt 18.500 Euro rechtskräftig.

Die Höhe der Geldbuße orientiert sich an den Kriterien des Art. 83 DS-GVO. Infolge der beachteten wirtschaftlichen Situation des Unternehmens ist davon auszugehen,

[41] https://lsaurl.de/OHMietSelbstauskunft

dass die Geldbuße wirksam, verhältnismäßig und abschreckend ist (Art. 83 Abs. 1 DS-GVO).

16.4 Nachweis der Einwilligung bei mehreren Beteiligten

Erziehungsberechtigte teilten dem Landesbeauftragten mit, dass anlässlich einer Veranstaltung in einer Kindertagesstätte eine Fotoaufnahme ihres Kindes angefertigt und dieses im Nachgang von einem Unternehmen in einem Sozialen Netzwerk ohne ihre Einwilligung zu Werbezwecken weltweit verbreitet wurde. Die Veranstaltung fand im Rahmen einer Kooperation zwischen einem Unternehmen und einer Kindertagesstätte statt. Als Rechtsgrundlage wurde sich auf eine Einwilligung der Erziehungsberechtigten berufen.

Bei der Prüfung der vermeintlichen „Einwilligungserklärung“ stellte sich heraus, dass diese bestenfalls ein Informationsschreiben darstellte. Die Voraussetzungen einer datenschutzrechtlichen Einwilligung nach Art. 7 DS-GVO lagen in dieser Erklärung nicht vor. Damit war für die Anfertigung und Veröffentlichung der Fotografien keine Rechtsgrundlage vorhanden.

Das Unternehmen negierte die Verantwortung hinsichtlich der fehlenden Rechtsgrundlage für die Fertigung und Veröffentlichung der Fotografie. Es habe sich auf die Kindertagesstätte verlassen. Diese habe erklärt, dass eine wirksame Einwilligung der Erziehungsberechtigten vorläge. Eine Vorlage und eine Kontrolle der Einwilligungserklärungen erfolgte seitens des Unternehmens allerdings nicht.

Der Landesbeauftragte verwies hier zunächst darauf, dass das Unternehmen verantwortlich ist für die Veröffentlichung der Fotografie im Sinne des Art. 4 Nr. 7 DS-GVO, weil es über den Zweck (Werbung) und die Mittel (Veröffentlichung im Sozialen Netzwerk) der Verarbeitung entschied. Denn ein Mitarbeiter des Unternehmens hatte die Fotoaufnahme angefertigt und in einem Sozialen Netzwerk veröffentlicht. Somit trug das Unternehmen die Verantwortung dafür, dass die Veröffentlichung des Fotos auf einer Rechtsgrundlage beruhte. Einzig mögliche Rechtsgrundlage wäre hier die Einwilligung gewesen, die aber nicht vorlag. Die Veröffentlichung war damit rechtswidrig.

Auch der Hinweis auf die Erklärung der Kindertagesstätte half hier nicht. Denn der Verantwortliche muss die Einhaltung der datenschutzrechtlichen Grundsätze (Art. 5 Abs. 2 DS-GVO) nachweisen können, wenn er sich auf eine Einwilligung beruft, dass die betroffene Person oder wie hier die Erziehungsberechtigten tatsächlich eingewilligt haben. Um diesen Nachweis zu erbringen, reicht es bei weitem nicht aus, sich auf mündliche allgemeine Erklärungen Dritter zu verlassen. Hier wäre es für das Unternehmen erforderlich gewesen, den Inhalt der behaupteten Einwilligungshandlung zu erfragen und zu prüfen, ob hier tatsächlich eine Einwilligung zur beabsichtigten Verarbeitung vorliegt.

16.5 Grenzen zulässiger Werbung durch bevollmächtigte Schornsteinfeger

Im Berichtszeitraum ging beim Landesbeauftragten eine Beschwerde über unzulässige Werbung ein.

Mehrere bevollmächtigte Bezirksschornsteinfeger hatten als solche Informationsschreiben an Privatpersonen verschickt. Dabei nannten sie in dem Briefkopf ihren Namen und ihre Adresse. Unter diesen Angaben führten sie die Bezeichnung „Schornsteinfegermeister“ auf.

Der Petent – ein anderer bevollmächtigter Bezirksschornsteinfeger – sah hierin einen Verstoß gegen wettbewerbsrechtliche und datenschutzrechtliche Bestimmungen in Form der unzulässigen Werbung.

Der Landesbeauftragte sah diesen Sachverhalt nicht als einen Fall von unzulässiger Werbung an. Die bloße Verwendung der Bezeichnung „Schornsteinfegermeister“ ohne weitere Angaben stellt kein Angebot von Dienstleistungen oder eine Form von Anpreisung dar. Nach § 45 Abs. 2 HwO handelt es sich um die Nennung einer beruflichen Qualifikation. Es waren hier auch keine sonstigen Hinweise auf einen Gewerbebetrieb zu erkennen.

Allerdings wies der Landesbeauftragte darauf hin, dass die Datenverarbeitung für öffentliche Zwecke – also für die Tätigkeit als bevollmächtigter Bezirksschornsteinfeger – strikt von der Datenverarbeitung für seine Tätigkeit als Schornsteinfegermeister getrennt werden muss.

Wird der bevollmächtigte Bezirksschornsteinfeger als solcher tätig, handelt er als öffentliche Stelle. Die hierfür in Form des Kehrbuchs verarbeiteten personenbezogenen Daten dürfen nach § 19 Abs. 1 und 5 SchfHwG nicht für andere Zwecke verwendet werden.

Auch § 7 Abs. 2 DSAG LSA sieht hier keine Möglichkeit einer zweckändernden Verwendung vor.

Betroffene Personen müssen darüber aufgeklärt werden, ob der Schornsteinfeger ihnen gegenüber öffentlich – also als bevollmächtigter Bezirksschornsteinfeger – oder als privater Unternehmer handelt. Der Zweck der jeweiligen Tätigkeit muss für die Betroffenen zweifelsfrei erkennbar sein. Die Informationspflichten aus Art. 13 DS-GVO (s. hierzu auch Nr. 14.3 im XVI. Tätigkeitsbericht) müssen getrennt erfüllt werden. Den Betroffenen muss entweder eine Datenschutzerklärung für die öffentliche Tätigkeit oder eine Datenschutzerklärung für die private unternehmerische Tätigkeit zur Verfügung gestellt werden.

16.6 Versand von personenbezogenen Daten per E-Mail durch Berufsgeheimnisträger

In mehreren Verfahren hatte der Landesbeauftragte zu beurteilen, ob der Versand von personenbezogenen Daten per unverschlüsselter E-Mail einen Verstoß gegen das Berufsgeheimnis darstellt.

Berufsgeheimnisträger sind z. B. Ärzte, Psychotherapeuten, Apotheker, Physiotherapeuten, Rechtsanwälte, Notare, Steuerberater, Sozialarbeiter sowie Beschäftigte von staatlich anerkannten Beratungsstellen und privaten Kranken-, Unfall- oder Lebensversicherungen.

Auch Berufsgeheimnisträger und die bei Ihnen Beschäftigten oder Mitwirkenden (z. B. Auftragsverarbeiter) unterliegen den Anforderungen aus Art. 5 Abs. 1 lit. f und Art. 32

DS-GVO. Deshalb müssen Sie für die Kommunikation per E-Mail ein angemessenes Schutzniveau gewährleisten.

Eine Transportverschlüsselung stellt regelmäßig eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen bei E-Mail-Kommunikation dar (s. auch Nr. 6.10).

Berufsgeheimnisträger sollten bei der Versendung von E-Mails mit personenbezogenen Daten deshalb grundsätzlich mindestens eine qualifizierte Transportverschlüsselung gewährleisten. Sofern E-Mail-Nachrichten besonders sensible Daten enthalten, sind eine qualifizierte Transportverschlüsselung und eine Ende-zu-Ende-Verschlüsselung notwendig.

Den Einwand, Patienten oder Mandanten seien mit einer unverschlüsselten E-Mail-Kommunikation einverstanden, wies der Landesbeauftragte zurück. Die Einwilligung nach Art. 7 DS-GVO bezieht sich auf die Verarbeitung personenbezogener Daten als solcher, nicht aber auf das Ergreifen von technischen Sicherheitsmaßnahmen. Dies gilt auch, falls Patienten oder Mandanten mit der unverschlüsselten E-Mail-Kommunikation von sich aus begonnen haben.

Berufsrechtliche Regelungen können die Vorschriften der DS-GVO nicht umgehen. Erlauben sie – wie z. B. § 2 Abs. 2 Satz 5 und 6 BORA – die unverschlüsselte Kommunikation per E-Mail, begeht der Berufsgeheimnisträger keinen berufsrechtlichen Verstoß, wenn er auf Verschlüsselung verzichtet. Ein Verstoß gegen datenschutzrechtliche Vorschriften bleibt aber möglich.

Allerdings sind eine qualifizierte Transportverschlüsselung und eine Ende-zu-Ende-Verschlüsselung nicht alternativlos. Daten könnten auch in einem nach dem aktuellen Stand der Technik sicher verschlüsselten Anhang mit einer obligatorisch transportverschlüsselten E-Mail übermittelt werden.

Wer gegenüber Mandanten oder Patienten auf den Versand von E-Mails verzichten möchte, könnte relevanten Schriftverkehr auch in einer datenschutzkonformen Cloud in Form eines Mandanten-Accounts mit entsprechenden Zugriffsrechten der Mandanten speichern.

16.7 Keine Zulässigkeit der Verarbeitung von Positivdaten durch Auskunfteien zur Feststellung der Wechselneigung von Kunden der Energieversorger

Laut Presseangaben werden in Deutschland immer mehr Verbraucher bei einem angestrebten Wechsel des Energieversorgers von diesem abgelehnt (Süddeutsche Zeitung, 9. September 2020, S. 15). Hintergrund dafür sollen auch Informationen der Energieversorger über ungestört verlaufende Vertragsverhältnisse und die bisherige Vertragslaufzeit sein (sog. Positivdaten). Laut Süddeutscher Zeitung und NDR planten die Auskunfteien Schufa (Sitz in Hessen) und CRIF Bürgel (Sitz in Bayern), die auch zahlreiche Daten von Bürgern aus Sachsen-Anhalt verarbeiten, Datenpools für Energieversorgungsunternehmen, die branchenweit Vertragsdaten der Kunden von Energieversorgern speichern und an anfragende Unternehmen übermitteln sollen. Insbesondere der Verbraucherzentrale Bundesverband e. V. (VZBV) befürchtete, dass Energieversorger aufgrund solcher Datenbanken künftig sehen könnten, dass Kunden schon häufiger gewechselt haben, sie dann entweder ablehnen oder ihnen attraktive Konditionen vorenthalten. Laut einer aktuellen Stellungnahme der Bundesregierung

(BT-Drs. 19/23669, S. 3) ist aber der aktive Lieferantenwechsel erklärtes Ziel der Liberalisierung der Strom- und Gasmärkte.

Durch Beschluss vom 11. Juni 2018 wies die DSK bereits darauf hin, dass Handels- und Wirtschaftsauskunfteien die Verarbeitung von Positivdaten zu Privatpersonen grundsätzlich nicht auf die Grundlage des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO stützen können. Erforderlich sei eine Einwilligung, wobei hier hohe Anforderungen hinsichtlich der Freiwilligkeit zu erfüllen seien. Eine Ausnahme bestehe für Kreditinstitute aufgrund spezieller Verpflichtungen zur Bonitätsprüfung nach dem Kreditwesengesetz.

Für den Bereich der Energieversorger ist eine solche Ausnahme nicht ersichtlich. Jeder Kunde hat das Recht, den für ihn günstigsten Energieversorger am Markt zu nutzen. Es war gerade Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen Wettbewerb zu ermöglichen. Vertragstreue Kunden dürfen zurecht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die gegebenenfalls ihre Möglichkeiten einschränkt, am Markt frei agieren zu können (siehe Beschluss der DSK vom 15. März 2021). Damit stehen der Verarbeitung von Positivdaten durch Auskunfteien zumindest überwiegende schutzwürdige Interessen der Kunden der Energieversorger entgegen.

17 Videoüberwachung

17.1 Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

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

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

Durch die Orientierungshilfe erhalten Verantwortliche und betroffene Personen ausführliche Informationen über die Voraussetzungen für eine datenschutzgerechte Videoüberwachung in den unterschiedlichsten Bereichen und über die Betroffenenrechte. Als Schlusskapitel enthält die Orientierungshilfe für Betreiber eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung. Als Anhang

[42] https://lsaurl.de/edpbvideoguidelines

finden sich Muster für Hinweisschilder, die es den Verantwortlichen erleichtern, den Transparenzpflichten gem. Art. 12 ff. DS-GVO nachzukommen.

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

17.2 Videoüberwachung im Nachbarschaftsbereich

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

Mitunter wird dem Landesbeauftragten von den Betreibern einer Videoanlage entgegengehalten, die Videoüberwachung, die von Privatgrundstücken ausgehe, sei Privatsache. Die Vorgaben der DS-GVO sind jedoch nur dann nicht anwendbar, wenn die mit der Videoüberwachung einhergehende Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt, Art. 2 Abs. 2 lit. c DS-GVO. Diese sogenannte „Haushaltsausnahme“ muss jedoch nach der Rechtsprechung des EuGH gerade im Bereich der Videoüberwachung eng ausgelegt werden. Sie greift z. B. nicht, wenn Aufnahmen des eigenen Grundstücks im Internet veröffentlicht werden und Dritte darauf erkennbar sind. Auch wenn die Videoüberwachung nur teilweise einen öffentlich zugänglichen Raum erfasst und dem Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses dient, ist die DS-GVO anwendbar.[44]

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

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

---

[43] https://lsaurl.de/VideoOH

[44] vgl. EuGH, Urteil v. 11. Dezember 2014, Rechtssache C-212/13

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

17.3 Datenschutzgerechter Einsatz von Drohnen

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

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

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

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

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

[45] https://lsaurl.de/VideoPrivat

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

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

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

17.4 Gesichtserkennung mithilfe von Videotechnik

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

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

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

[46] https://lsaurl.de/Drohnen

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

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

18 Bußgeldverfahren

18.1 Statistik der behördlichen Bußgeldverfahren

Datenschutzrechtliche Verstöße kann der Landesbeauftragte mit einem Bußgeld gemäß Art. 83 Abs. 4 bis 6 DS-GVO ahnden (§§ 23 Abs. 5, 31 DSAG LSA i. V. m. § 41 BDSG). In diesem Sinne wurden 17 Bußgeldverfahren eingeleitet, davon ein Verfahren eingestellt und zehn Verfahren im Jahr 2020 rechtskräftig abgeschlossen.

Vermehrt wurden Ordnungswidrigkeitsverfahren wegen unzulässiger Videoüberwachung von Beschäftigten aus den Bereichen des Einzelhandels und der Gastronomie eingeleitet. Bei der Bußgeldbemessung wurde berücksichtigt, dass die Geschäftstätigkeit durch die staatlichen Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt ab März ganz erheblich beeinträchtigt war.

Die Gesamtsumme der rechtskräftig verhängten Bußgelder aus Verfahren, die in den Jahren 2019 und 2020 begannen, beläuft sich auf 20.650 Euro:

Tatbestände	Bußgelder insgesamt
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Datenverarbeitung	7.300 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Videoüberwachung von Beschäftigten	1.100 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6, 9 DS-GVO Unzulässige Verarbeitung von Daten besonderer Kategorien	600 Euro
Art. 83 Abs. 5 lit. b i. V. m. Art. 15, 12 DS-GVO Verspätete Informationserteilung	1.500 Euro

Art. 83 Abs. 4 lit. a i. V. m. Art. 25 Abs. 1 DS-GVO Unzureichender Datenschutz durch Technikgestaltung	9.000 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 31 DS-GVO Unzureichende Zusammenarbeit mit der Aufsichtsbehörde	1.150 Euro

Zum Zeitpunkt der Erstellung dieses Tätigkeitsberichtes wurde ein Verfahren gegen ein Wohnungsunternehmen vor dem Amtsgericht Magdeburg abgeschlossen. Die Verfahrenseinleitung erfolgte bereits im Jahr 2019 wegen unzulässiger Erhebung und Speicherung personenbezogener Daten von mietinteressierten Personen. Bezüglich der Sach- und Rechtslage sowie der Bußgeldhöhe wird auf den Bericht zu Nr. 16.3 „Kontrolle eines Wohnungsunternehmens aufgrund anonymer Mitteilung“ verwiesen. Dieses Bußgeld ist allerdings in der oben genannten Tabelle nicht enthalten.

18.2 Gerichtliche Zuständigkeit bei OWi

Mit dem „Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens“ (BR-Drs. 107/20(B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte gemäß § 41 Abs. 1 Satz 3 BDSG für Geldbußen nach der DS-GVO über 100.000 Euro streichen. Unabhängig von der Bußgeldhöhe sollen die Amtsgerichte nach § 41 BDSG i. V. m. § 68 OWiG über sämtliche Einsprüche entscheiden. Nach Einschätzung des Landesbeauftragten verkennt der Gesetzentwurf in eklatanter Weise die besondere wirtschaftliche, technische und rechtliche Komplexität der Verhängung von Geldbußen nach der DS-GVO. Die Vorschriften der DS-GVO sind eng am EU-Kartellrecht orientiert. In Kartell-Ordnungswidrigkeitsverfahren entscheiden auf nationaler Ebene die Oberlandesgerichte (§ 83 GWB). Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte noch stärker als bisher belasten. Darauf weist auch die Entschließung „Datenschutz braucht Landgerichte auch erstinstanzlich“ der DSK vom 22. September 2020 **(Anlage 6)** hin.

18.3 Weiterentwicklung des Bußgeldkonzeptes, Behördliche Praxis

Das von der DSK am 14. Oktober 2019 veröffentlichte Bußgeldkonzept knüpft an die Struktur der Festsetzung von Geldbußen gem. EU-Kartellrecht[47] (Az. 2006/C 210/02) an. Danach wird ein umsatz- und tatbezogener Grundbetrag ermittelt, der infolge erschwerender bzw. mildernder Umstände entweder erhöht oder reduziert wird. Da nicht von allen Unternehmen die Umsatzhöhen bekannt sind, behilft sich das Bußgeldkonzept mit Startbeträgen nach „Unternehmenskategorien“, die im nächsten Schritt tatbezogen bewertet werden. Aus der Wirtschaft und von einzelnen Aufsichtsbehörden kam erhebliche Kritik wegen des starken Umsatzbezuges, der regelmäßig zu sehr hohen Geldbußen führt. Diese Kritik teilte das LG Bonn mit Urteil vom 11. November 2020 zum Verfahren des BfDI gegen das Telekommunikationsunternehmen „1&1“ (Az. 29 OWI 1/20), indem es das Konzept für leichte Verstöße bei umsatzstarken Unternehmen für nicht anwendbar hält. Gleiches gilt für schwere Verstöße von umsatzschwa-

[47] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:210:0002:0005:DE:PDF

chen Unternehmen. Insofern besteht Anlass für die DSK und ihren Arbeitskreis „Sanktionen“ das Konzept weiterzuentwickeln. Erste Versionen lagen zum Zeitpunkt der Erstellung dieses Tätigkeitsberichtes bereits vor.

Parallel wird vom EDSA gem. Art. 70 Abs. 1 lit. k DS-GVO an einer Leitlinie („Fining Guidelines“) für die Aufsichtsbehörden in Bezug auf die Festsetzung von Geldbußen nach Art. 83 DS-GVO gearbeitet. Mit der Vorlage einer solchen Leitlinie kann wohl erst Anfang 2022 gerechnet werden.

Für die Bußgeldbemessung durch den Landesbeauftragten ist das Bußgeldkonzept eine wertvolle Hilfestellung. Infolge der Pandemie wurde bei betroffenen Unternehmen allerdings berücksichtigt, dass deren Geschäftstätigkeiten durch die staatlichen Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt ab März ganz erheblich beeinträchtigt waren. Die wirtschaftliche Situation war glaubhaft zu machen bzw. durch geeignete Unterlagen nachzuweisen.

18.4 Schutz von Whistleblowern im Bußgeldverfahren

Wichtig für den Landesbeauftragten ist der Schutz von beschwerdeführenden Personen, die ihren Namen zwar angeben, aber nach außen anonym bleiben möchten. Häufig sind dies Personen, die von dem verantwortlichen Unternehmen abhängig beschäftigt sind, und bei Offenlegung ihres Namens mit Repressalien rechnen. Die Angabe der Kontaktdaten gegenüber dem Landesbeauftragten kann aber sehr vorteilhaft sein, damit die Person zur weiteren Sachverhaltsaufklärung beitragen kann und selbst über den Fortgang informiert wird.

Im Falle eines Antrages auf Akteneinsicht durch den Verantwortlichen im Verwaltungsverfahren werden unter Anwendung des § 13 Abs. 3, 6 BDSG, Art. 54 Abs. 2 DS-GVO sowie unter Berufung auf das Urteil des BVerwG vom 4. September 2003 (Az. 5 C 48/02) personenbezogene Daten der beschwerdeführenden Person geschwärzt, sofern die Person anonym bleiben möchte.

Genauso verhält sich der Landesbeauftragte auch im Bußgeldverfahren. Europäisch betrachtet stellt die Geldbuße nach Art. 83 DS-GVO eine verwaltungsrechtliche Sanktion dar (ErwGr 150). Insofern sind die Regelungen des Strafverfahrens nach § 147 StPO i. V. m. § 46 OWiG, § 41 BDSG eher restriktiv auszulegen, soweit nicht die fundamentalen Rechte der beschuldigten Person auf ein faires Verfahren nach Art. 6 EMRK betroffen sind. Der EU-Gesetzgeber beabsichtigt selbst einen starken Schutz der hinweisgebenden Person wie z. B. in Art. 23 Abs. 1 lit. i 2. Alt., Art. 54 Abs. 2 DS-GVO und Art. 15 Abs. 1 lit. e, 16 Abs. 4 lit. e, Art. 44 Abs. 2 Satz 2 RL 2016/680. In diesem Sinne werden im Falle der Akteneinsicht in die Bußgeldakte personenbezogene Daten der beschwerdeführenden Person nicht offengelegt, sofern die Person dies nicht möchte.

Anders ist die Situation, wenn neben den Angaben der beschwerdeführenden Personen trotz Sachverhaltsuntersuchung keine anderen Beweismittel für das Vorliegen eines datenschutzrechtlichen Verstoßes zur Verfügung stehen. Dann befragt der Landesbeauftragte die beschwerdeführende Person, ob nach wie vor Bedenken gegen die Offenlegung des Namens bestehen.

Anlagen

Anlage 1

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2020

Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

- Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

- Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die weniger, oder – wie eine vorherige Anonymisierung – sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.

- Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. **Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

Anlage 2

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 16. April 2020

Polizei 2020 – Risiken sehen, Chancen nutzen!

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten „fachlichen Bebauungsplan“ für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

1. Umfassende Bestandsaufnahme

Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken

Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerte- und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste“ zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung“, ein „Basisdienst Datenqualität“ und ein „Basisdienst Aufsicht und Kontrolle".

Anlage 3

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. August 2020

Registermodernisierung verfassungskonform umsetzen!

Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz – RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll u. a. eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.

Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12.09.2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.

Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potential der möglichen missbräuchlichen Verwendung.

So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks. Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.

Die Datenschutzkonferenz hatte demgegenüber „sektorspezifische“ Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.

Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf „rechtliche, technische und organisatorische Komplexität“ abgelehnt.

Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den „Eilbedarf“ unter den Tisch fallen zu lassen.

Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

Anlage 4

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 1. September 2020

Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen.

Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden. Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der EPA, d. h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte (Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d. h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible

persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs. 164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

Anlage 5

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 22. September 2020

Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[48] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[49] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten.“ Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

---

[48] Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

[49] PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,

- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und

- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:

    - Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.

    - Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.

    - Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:

    - Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.

3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

    - Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:

    - Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.

    - Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:

    - Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam

und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

Anlage 6

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 22. September 2020

Datenschutz braucht Landgerichte auch erstinstanzlich

Mit dem *„Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens“* (BR-Drs. 107/20 (B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen nach der Datenschutz-Grundverordnung (DSGVO) über 100.000 Euro streichen. Selbst über Geldbußen in dieser Höhe sollen künftig die Amtsgerichte entscheiden.

Das Ziel der Effektivierung des Bußgeldverfahrens wird mit dem geplanten Gesetz jedoch nicht erreicht werden. Der Gesetzentwurf verkennt in eklatanter Weise die besondere wirtschaftliche, technische und rechtliche Komplexität von DSGVO-Geldbußen. Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte zudem nicht etwa entlasten, sondern noch stärker als bisher belasten.

Das Sanktionsrecht der DSGVO ist – anders als der Bundesrat unterstellt – mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Datenschutz-Ordnungswidrigkeiten mit Geldbußen über 100.000 Euro weisen wirtschaftlich und technisch eine besondere Komplexität auf und bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind viel eher mit Wirtschaftsstrafsachen vergleichbar, die ohnehin den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DSGVO am Kartellrecht orientiert. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Abs. 2 Satz 1 Bundesdatenschutzgesetzes (BDSG) zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der Strafkammern als sog. große Bußgeldkammern entsprechend § 76 GVG vorsieht.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert daher die Beibehaltung der landgerichtlichen Zuständigkeit für DSGVO-Geldbußen über 100.000 Euro und warnt vor einer Streichung der Vorschrift und deren Folgen.

Anlage 7

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 25. November 2020

Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangsgesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das "Schrems II"-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten.

Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.

Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa

wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Art. 7 GRCh geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Art. 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Art. 10 GG und ergänzend durch das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.

Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integrer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integrer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

Anlage 8

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 25. November 2020

Betreiber von Webseiten benötigen Rechtssicherheit. Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen

Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie[50] vollständig und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) umzusetzen.

Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt hat.[51] Das Urteil des Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 – „Planet49“) verstärkt nach Auffassung der DSK den seit langem bestehenden, dringenden Handlungsbedarf.

Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018“ den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der Datenschutz-Grundverordnung (DSGVO) nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.[52]

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Abs. 3 Telemediengesetz (TMG) wäre ein solches Vorgehen dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 ePrivacy-Richtlinie legt der

---

[50] Richtlinie 2002/58/EG in der letzten Änderung durch die Richtlinie 2009/136/EU

[51] Siehe Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5. Februar 2015, abrufbar unter: https://www.datenschutzkonferenzonline.de/media/en/20150205_en_Entschliessung_Cookies.pdf

[52] Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“, abrufbar unter: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html, Orientierungshilfe für Anbieter von Telemedien https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

BGH § 15 Abs. 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der BGH der Vorabentscheidung des Europäischen Gerichtshofes gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.

Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacy-Richtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene weitgehend abschließend durch die Datenschutz-Grundverordnung geregelt. Art. 5 Abs. 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Abs. 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.

§ 15 Abs. 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Abs. 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste u. a. in Bezug auf „Cookies“ rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen.

Anlage 9

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 25. November 2020

Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten

Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicherheitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.

Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs- und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vgl. BVerfG, o. g. Beschluss vom 27. Mai 2020,

Rn. 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.

Anlage 10

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 15. März 2021

„Energieversorgerpool“ darf nicht zu gläsernen Verbraucher*innen führen

Bei Auskunfteien und Energieversorgern gibt es Überlegungen, einen sog. Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollen auch Positivdaten der Kund*innen gespeichert und an andere Energieversorger übermittelt werden. Positivdaten sind Daten über Verträge, bei denen die Belieferten keinen Anlass zu Beanstandungen geben, sich also vertragskonform verhalten.

Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob Verbraucher*innen eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder etwa regelmäßig Angebote für Neukund*innen nutzen. Verbraucher*innen, die regelmäßig das für Sie kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden.

Jede Bürgerin und jeder Bürger hat jedoch das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche „Schnäppchenjäger“ in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und ggf. von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher*innen zu identifizieren und sie ggf. von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider.

Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund*innen. Vertragstreue Verbraucher*innen dürfen zu Recht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die ggf. ihre Möglichkeiten einschränkt, frei am Markt agieren zu können.

Die Speicherung und Übermittlung von Positivdaten durch einen Energieversorgerpool würde erheblich zu gläsernen Verbraucher*innen beitragen und wäre nach Art. 6 Absatz 1 Satz 1 lit. f) DS-GVO rechtswidrig.

Anlage 11

Organigramm

Stichwortverzeichnis

E

F

G

H

I