SACHSEN-ANHALT

XII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Dieser Text entspricht der Landtagsdrucksache 6/4812

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

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

Vorwort

Das Jahr 2015 kann als historisches Jahr für den Datenschutz bezeichnet werden: Es fand eine Einigung über die neue Europäische Datenschutz-Grundverordnung statt. Der Europäische Gerichtshof erklärte die Safe Habor-Regelung der Europäischen Kommission für unzulässig; die USA sind kein sicherer Datenhafen.

Gleichzeitig erfährt der Datenschutz durch Verschärfungen der Sicherheitspolitik infolge von Terroranschlägen und mit der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft zusätzliche Bewährungsproben.

Der XII. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2013 bis zum 31. März 2015. Bei einzelnen Beiträgen konnten noch darüber hinaus reichende aktuelle Sachstände einbezogen (Redaktionsschluss: 5. Februar 2016) und Entwicklungen in der Gesetzgebung bis zum Ende der 6. Legislaturperiode des Landtages von Sachsen-Anhalt berücksichtigt werden. Der Bericht knüpft an den XI. Tätigkeitsbericht (LT-Drs. 6/2602) an und bezieht auch die Entschließung des Landtages vom 5. Juni 2015 (LT-Drs. 6/4150) und die dazugehörige Stellungnahme der Landesregierung (LT-Drs. 6/4305) ein.

Der Datenschutzbericht dient der Unterrichtung des Landtages, zusammen mit der zum Bericht abzugebenden Stellungnahme der Landesregierung (§ 22 Abs. 4a Satz 1 und 2 DSG LSA; diese Regelung gilt auch für den Bereich der Tätigkeit des Landesbeauftragten als Aufsichtsbehörde nach § 38 BDSG, siehe § 22 Abs. 2 DSG LSA), der Öffentlichkeitsarbeit (§ 22 Abs. 4a Satz 3 DSG LSA), der Information der Behörden, Unternehmen und anderen verantwortlichen privaten Stellen, der Datenschutzbeauftragten in Behörden und Unternehmen und interessierter Bürgerinnen und Bürger.

Inhaltlich geht es auch im aktuellen Bericht um Konzeptionen und Maßnahmen des Datenschutzes in den vier Bereichen Recht, Technik, Datenschutzkontrolle und Medienkompetenz.

Der Bericht greift wiederum datenschutzpolitische Themen auf; dazu wird auch auf die im Anlagenteil aufgenommenen Entschließungen verwiesen. Er behandelt vielfältige rechtliche und technische Entwicklungen und stellt Materialien und Hinweise aus der Praxis für die Praxis anhand ausgewählter anschaulicher Einzelfälle, Beratungen und Kontrollen zur Verfügung.

Mein besonderer Dank gilt wieder meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle.

Magdeburg, den 5. Februar 2016

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

Inhaltsverzeichnis

Anlagenverzeichnis

Nationale Datenschutzkonferenz

Düsseldorfer Kreis

Europäische Datenschutzkonferenz

Internationale Datenschutzkonferenz

Weitere Dokumente

Abkürzungsverzeichnis

A

ABl.	Amtsblatt
AEPD	Agencia Española de Protección de Datos
AES	Advanced Encryption Standard
AG	Arbeitsgruppe(n)
AntiDopG	Gesetz zur Bekämpfung von Doping im Sport
AO	Abgabenordnung
App	engl. Kurzform für „Application Software“ (Anwendungssoftware
Apps	Applikationen
ArchG LSA	Archivgesetz des Landes Sachsen-Anhalt
ATDG	Antiterrordateigesetz

B

BAG	Bundesamt für Güterverkehr
BAGE	Entscheidungen des Bundesarbeitsgerichts
BArchG	Bundesarchivgesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BIC	Business Identifier Code (Geschäftsstellen-Kennung)
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e. V.
BMG	Bundesmeldegesetz
BMG-AG LSA	Ausführungsgesetz des Landes Sachsen-Anhalt zum Bundesmeldegesetz
BMI	Bundesministerium des Innern
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Ministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BYOD	Bring Your Own Device („Bring dein eigenes Gerät mit“)
BZRG	Bundeszentralregistergesetz

C

CA	Certificate Authority (Zertifizierungsstelle)
CBP	College Bescherming Persoonsgegevens
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIO	Chief Information Officer (Leiter Informationstechnologie)

CNIL	Commission Nationale de l'Informatique et des Libertés
CoC	Code of Conduct
CPS	Cyber-Physisches System (engl. cyber-physical system)
CVE	Common Vulnerabilities and Exposures

D

DANE	DNS-based Authentication of Named Entities (Protokoll, um digitale Zertifikate über das Domain Name System bekannt zu geben)
Dataport	Anstalt des öffentlichen Rechts, Hauptsitz Altenholz, Schleswig-Holstein
DCS	Data Center Steuern von Dataport in Rostock
DDR	Deutsche Demokratische Republik
DEHOGA	Deutscher Hotel- und Gaststättenverband e. V.
Device Fingerprinting	digitaler Fingerabdruck einer Systemkonfiguration
DFN	Deutschen Forschungsnetz
DIN	Deutsches Institut für Normung
DME	Dynamic Mobile Exchange™, der dänischen Firma Excitor
DNS	Domain Name System, Standard zur Namensvergabe im Internet
DNSSEC	Domain Name System Security Extensions – eine Reihe von Internetstandards, die das Domain Name System (DNS) um Sicherheitsmechanismen zur Gewährleistung der Authentizität und Integrität der Daten erweitern
DPI	Deep Packet Inspection
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DS GVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
DVBl	Deutsches Verwaltungsblatt

E

eAkte	elektronische Akte
eGK	elektronische Gesundheitskarte
EGovG	E-Government-Gesetz
eID	elektronischer Identitätsnachweis
eIDAS VO	Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EnWG	Energiewirtschaftsgesetz
ERV	Elektronischen Rechtsverkehr
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen

F

FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit

FATCA	Foreign Account Tax Compliance Act
FE-Schrift	Fälschungserschwerende Schrift
FFOG	Feld- und Forstordnungsgesetz
FIM	Föderales Informationsmanagement
FITKO	Föderale IT-Kooperation

G

GB	Gigabyte
GewO	Gewerbeordnung
GG	Grundgesetz
GIAZ	Gemeinsames Informations- und Abwehrzentrum im Landeskriminalamt Sachsen-Anhalt
GIW-Kommission	Kommission für Geoinformationswirtschaft des Bundesministeriums für Wirtschaft und Energie
GKVS	Gemeinsamen Konferenz der Verkehrs- und Straßenbauabteilungsleiter der Länder
GPS	Global Positioning System
GVBl. LSA	Gesetz und Verordnungsblatt des Landes Sachsen-Anhalt

H

HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
HbbTV	Hybrid broadcast broadband TV
HeizkostenV	Verordnung über Heizkostenabrechnung
HGB	Handelsgesetzbuch
HTTPS	HyperText Transfer Protocol Secure

I

IBAN	International Bank Account Number (internationale Bankkontonummer)
IDE	Integrated Drive Electronics (integrierte Laufwerkselektronik)
IDS	Intrusion Detection System
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikationstechnologie
IMEI	International Mobile Station Equipment Identity (eindeutige 15-stellige Seriennummer für Mobilfunk-Endgeräte)
InfrAG	Infrastrukturabgabengesetz
IoT	Internet der Dinge (engl. Internet of Things)
IP-Adresse	Internetprotokoll-Adresse
IQB	Institut zur Qualitätsentwicklung im Bildungswesen
ISA	Informationssystem Sachsen-Anhalt
IT	Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
ITN-XT	Informationstechnisches Netz Sachsen-Anhalt „eXTended“ (erweitert)
IT-PLR	IT-Planungsrat
IZG LSA	Informationszugangsgesetz des Landes Sachsen-Anhalt

J

JVA	Justizvollzugsanstalt
JVollzGB	Justizvollzugsgesetzbuch Sachsen-Anhalt

K

KBA	Kraftfahrt-Bundesamt
KFRG	Krebsfrüherkennungs- und -registergesetz
Kfz	Kraftfahrzeug
Kita	Kindertagesstätte
KraftStG	Kraftfahrzeugsteuergesetz
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photografie
KVG LSA	Kommunalverfassungsgesetz des Landes Sachsen-Anhalt

L

LAN	Local Area Network – lokales Netzwerk
LG	Landgericht
LJagdG	Landesjagdgesetz für Sachsen-Anhalt
LKA	Landeskriminalamt
Lkw	Lastkraftwagen
LT-Drs.	Landtags-Drucksache
LuftVG	Luftverkehrsgesetz
LuftVO	Luftverkehrs-Ordnung
LVermGeo	Landesamt für Vermessung und Geoinformation

M

MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MDK	Medizinischer Dienst der Krankenversicherung
MEID	Mobile Equipment Identifier (Mobilgerät-Kennung)
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MG LSA 2015	Entwurf Meldegesetz des Landes Sachsen-Anhalt 2015
MiLoG	Gesetz zur Regelung eines allgemeinen Mindestlohns (Mindestlohngesetz)
MLV	Ministerium für Landesentwicklung und Verkehr
MMS	Multimedia Messaging Service (Erweiterung von SMS, Versand multimedialer Inhalte und längerer Nachrichten)
MVollzG	Maßregelvollzugsgesetz

N

NADA	Nationale Anti-Doping Agentur Deutschland
NEGS	Nationale E-Government-Strategie
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report
nPA	neuer Personalausweis
NSA	National Security Agency (Nationale Sicherheitsbehörde der USA)
NSU	Nationalsozialistischer Untergrund
NZA	Neue Zeitschrift für Arbeitsrecht

O

OAA	Open Automotive Alliance
OSCI	Online Services Computer Interface
OVG	Oberverwaltungsgericht

P

PC	Personalcomputer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PGP	Pretty Good Privacy (Name eines Verschlüsselungssystems)
PKI-LSA	Public Key Infrastructure Land Sachsen-Anhalt
Pkw	Personenkraftwagen
PPP	Public Private Partnership
PROMIS	Personal-, Ressourcen-, Organisationsmanagement- und Informationssystem für das Land Sachsen-Anhalt
PwC	PricewaterhouseCoopers International Limited

Q

QES	Qualifizierte Elektronische Signatur

R

RFC	Requests for Comments – „Bitte um Kommentare“ sind Internet-Dokumente und -Standards
RHESA	Regionales Herzinfarkregister Sachsen-Anhalt
RiMS-LSA	Risikomanagement für besonders rückfallgefährdete Sexualstraftäter im Land Sachsen-Anhalt
Rn.	Randnummer

S

SATA	Serial Advanced Technology Attachment (fortgeschrittene serielle Anschlusstechnologie)
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SD-Karte	Secure Digital Memory Card (sichere digitale Speicherkarte
SEPA	Single Euro Payments Area (einheitlicher europäischer Zahlungsverkehrsraum)
SGB	Sozialgesetzbuch
SIM	Subscriber Identity Module (dt.: Teilnehmer-Identitätsmodul, umgangssprachlich: Handy-Chipkarte)
S/MIME	Secure Multi Purpose Internet Mail Extension
SIS II	Schengener Informationssystem II
SMS	Short Message Service (dt.: Kurznachrichtendienst, Länge max. 160 Zeichen)
SMTP	Simple Mail Transfer Protocol – Verfahren zum Versenden von E-Mails
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SpielbG LSA	Spielbankgesetz des Landes Sachsen-Anhalt
SRIW	Selbstregulierung Informationswirtschaft e. V.
SSL	Secure Sockets Layer (Sicherheitsprotokoll)

StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVO	Straßenverkehrs-Ordnung
SÜG-LSA	Sicherheitsüberprüfungs- und Geheimschutzgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication

T

TaskForce	Arbeitsgruppe
TFG	Transfusionsgesetz
TISA	Trade in Service Agreement
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security (Sicherheitsprotokoll)
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TMG	Telemediengesetz
TTIP	Transatlantic Trade and Investment Partnership
TV	Television (Fernsehen)

U

UKlaG	Unterlassungsklagengesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USA	United States of America (Vereinigte Staaten von Amerika)
USB	Universal Serial Bus (universelles serielles Bussystem)

V

VDA	Verband der deutschen Automobilindustrie
VEMAGS	Verfahrensmanagement für Großraum- und Schwertransporte
VermGeoG LSA	Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt
VG	Verwaltungsgericht
VPN	Virtual Private Network (virtuelles privates Netzwerk)
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

W

WADA	Welt-Anti-Doping-Agentur
WLAN	Wireless Local Area Network
WTG LSA	Wohn- und Teilhabegesetz
WTG-MitwVO	Wohn- und Teilhabegesetz-Mitwirkungsverordnung
WTG-PersVO	Wohn- und Teilhabegesetz-Personalverordnung

Z

ZensG 2011	Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011)
ZD	Zeitschrift für Datenschutz
ZMDB	Zentraler Meldedatenbestand auf Landesebene

ZMGR	Zeitschrift für das gesamte Medizin- und Gesundheitsrecht
ZPO	Zivilprozessordnung

1 Entwicklung und Situation des Datenschutzes

Im Folgenden werden einleitend aktuelle Entwicklungen aufgegriffen und näher beschrieben, bei denen besondere Herausforderungen für die Datenschutzgrundrechte und die dem Landesbeauftragten zugewiesenen Befugnisse bestehen. Gefährdungen für und Eingriffe in die Privatsphäre resultieren aus der fortschreitenden Digitalisierung aller Lebensbereiche. Überwachung, Steuerung und Kontrolle des Verhaltens der Menschen nehmen zu. Dies gilt im Bereich der inneren Sicherheit ebenso wie im Verbraucheralltag und in der Wirtschaft. Recht und Technik können die Entwicklungen nur unzureichend kompensieren. Defizite gibt es auch bei der Medienbildung. Anspruch und Wirklichkeit des Datenschutzes treiben weiter auseinander. Eine der Zukunftsfragen lautet: Kann das Big Data-Prinzip mit dem Grundsatz der Datensparsamkeit harmonisiert werden?

Hoffnung machen drei maßgebliche Entscheidungen des Europäischen Gerichtshofes der letzten Zeit: Zur Unzulässigkeit der Vorratsdatenspeicherung, zum „Recht auf Vergessen“ und zur Datenübermittlung von der EU in die USA. Die neue Europäische Datenschutz-Grundverordnung dürfte hingegen nicht alle Datenschutzwünsche erfüllen.

Informationelle Selbstbestimmung als Teil des Persönlichkeitsrechts ist weiterhin Funktionsbedingung der freiheitlichen Demokratie und insofern einer ihrer wesentlichen Maßstäbe. Wenn dies nicht hinreichend beachtet wird, nimmt das Gemeinwohl Schaden.

1.1 Sicherheit und Freiheit

In den vorangegangenen Tätigkeitsberichten (siehe jeweils Nr. 1.1) sind unter Heranziehung der Rechtsprechung des Bundesverfassungsgerichtes maßgebliche Grundsätze und Gebote für die Abwägung zwischen Sicherheit und Freiheit beschrieben worden: Primat der Freiheit, Bindung des Staates an das Rechtsstaatsgebot bei der Wahrnehmung seines Schutzauftrages, Unzulässigkeit eines Sicherheitsverständnisses des Staates als Präventionsstaat, kein Rechtfertigungsdruck für das Verbergen der Privatsphäre, Gebot der Überwachungsgesamtrechnung durch den überwachenden Staat, Evaluation bzw. Überprüfung vorhandener Überwachungsmaßnahmen, Technikfolgenabschätzung, Trennung zwischen polizeilicher und nachrichtendienstlicher Tätigkeit.

Im Falle von akuten Gefährdungen der inneren Sicherheit und Angriffen auf Freiheitsgrundrechte etwa durch konkrete Anschläge wird der Datenschutz oftmals als Verhinderungsinstrument wirksamer Kriminalitäts- und Terrorbekämpfung diffamiert und als vermeintlicher Täterschutz kritisiert. Das Grundrecht auf informationelle Selbstbestimmung ist jedoch Teil der Verfassungsordnung, ja Teil der Verfassungsidentität. Daraus ergibt sich auch das Verbot einer Totalüberwachung. Stets kommt es auf die strikte Beachtung des Verfassungsgrundsatzes der Verhältnismäßigkeit an (siehe dazu die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015, **Anlage 29**).

Die Zusammenarbeit von NSA und BND steht seit langem in der Kritik. Die Nutzung von Selektoren bzw. Suchbegriffen der NSA durch den BND und die Weitergabe von Daten in die USA erscheint auch nach den vorläufigen Ergebnissen des betreffenden Bundestagsuntersuchungsausschusses übermäßig, unverhältnismäßig und unzulässig. Die Bundesregierung plant spät, durch gesetzliche Regelungen Kontrollmechanismen insbesondere zugunsten des Bundestages einzubauen. Wirtschaftsspionage durch den BND soll ausgeschlossen sein. Insgesamt sind die Konsequenzen aus den Enthüllungen von Edward Snowden über die Internetüberwachungen durch US-amerikanische und britische Geheimdienste noch nicht angemessen gezogen worden.

Der Landesbeauftragte war zusammen mit der Staatskanzlei als Hausherr und der Beauftragten des Landes Sachsen-Anhalt für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR sowie dem Direktor der Landeszentrale für Politische Bildung Gastgeber einer Diskussionsveranstaltung im November 2015 zum Thema „25 Jahre Deutsche Einheit – Was sind uns Freiheit, Demokratie und Grundrechte noch wert?“ Der Landesbeauftragte betonte dabei die Unterschiede zwischen der Diktatur und dem „Unrechtsstaat“ DDR mit dem Geheimdienst der Staatssicherheit einerseits und dem Rechtsstaat USA mit dem Geheimdienst NSA andererseits. Neben gleichwohl berechtigter Kritik an dem übermäßigen Datensammeln der NSA seien auch die Überwachungen in Europa auf den Prüfstand zu stellen. Die Abwägung im Verhältnis von Freiheit und Sicherheit dürfe nicht die Menschenwürde abwerten. Keine zulässige Antwort ist die Feststellung, dass die eigentliche Bedrohung im Rechtsstaat nicht vom Staat ausgehe, und man daher der Gefahrenabwehr Vorrang einräumen müsse. Denn bei den allermeisten Menschen geht es gar nicht um Gefahrenabwehr, schon gar nicht um Terrorabwehr, sondern um eine vorsorgliche Vorfeldüberwachung weit vor einem eventuellen Verdacht einer auch nur eventuellen Gefährdung. In Demokratien müssen Geheimdienste ausgleichender Kontrollsysteme unterworfen werden. Es gilt das Prinzip: Vertrauen ist gut, Kontrolle ist besser.

Der Kern des Konflikts zwischen Sicherheit und Freiheit wird bei anlasslosen Massenüberwachungen wie der Vorratsdatenspeicherung, die zu einer Totalüberwachung führen kann, in besonderer Weise deutlich.

Im maßgeblichen Urteil des EuGH vom 8. April 2014 (siehe Näheres unter Nr. 7.1) wird wie schon zuvor im Urteil des Bundesverfassungsgerichts vom 2. März 2010 das Gefühl des Überwachtwerdens des Privatlebens als besonders auffällig hervorgehoben. Zwar ist die Bekämpfung des internationalen Terrorismus und schwerer Kriminalität ein legitimes Ziel und eine Vorratsspeicherung insofern durchaus nützlich. Jedoch fehlt es an der Beachtung der Verhältnismäßigkeit. Der EuGH beschreibt den Umstand anlassloser Massenüberwachung wie folgt:

„Die (angegriffene) *Richtlinie über die Vorratsspeicherung betrifft zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. […] Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer*

Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten."

Die Freiheitsgrundrechte werden weiter vernachlässigt. Die Bekämpfung von Kriminalität und Terrorismus, die oft nur Vorwand ist, führt zu mehr Datensammlungen und Überwachungen. Dies ist ein wesentlicher Grund, warum nicht nur das Datengebaren der Wirtschaft und insbesondere internationaler Internetkonzerne in der Kritik stehen muss (vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014, **Anlage 14**), sondern stets auch das Handeln des bzw. der Staaten selbst. Big Data-Anwendungen enthalten in beiden Bereichen hohe Risiken. Eine aktuelle Entwicklung in diesem Zusammenhang betrifft Auswertungsmöglichkeiten wie das sogenannte Predictive Policing, bei dem Kriminalitätsschwerpunkte mittels Big Data-Analyse vorhergesagt werden (siehe Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015, **Anlage 23**).

1.2 Verbraucherdatenschutz – Befugnisse als Aufsichtsbehörde

Eine Stärkung des Verbraucherdatenschutzes (siehe bereits XI. Tätigkeitsbericht, Nr. 1.2) kann sich aus einem neuen Projekt der Verbraucherzentralen ergeben. Diese haben in den Bereichen "Finanzmarkt" und „Digitale Welt" eine sogenannte Marktwächterfunktion übernommen. Insbesondere der Marktwächter „Digitale Welt" weist Berührungspunkte zum Datenschutz auf. Er kann als Frühwarnsystem bezüglich Datenschutzverstößen bei Telekommunikationsdienstleistungen, elektronischen und mobilen Geschäftsabwicklungen, digitalen Gütern und Dienstleistungen (z. B. Vergleichsportalen) sowie nutzergenerierten Inhalten fungieren. Daher ist eine Kooperation mit den Datenschutzbehörden beabsichtigt. Diese sollen über die Erkenntnisse des Marktwächters informiert werden. Vorsitzende des Beirats des Marktwächters „Digitale Welt" ist die Landesbeauftragte für den Datenschutz Brandenburg. Verbraucher haben jetzt die Möglichkeit, Beschwerden über den Verbraucher(daten)-schutz mitzuteilen[1]. Der Landesbeauftragte begrüßt die Einrichtung des Marktwächters und wird im Übrigen seine gute Zusammenarbeit mit der Verbraucherzentrale Sachsen-Anhalt e. V. fortsetzen.

Seit dem 1. Oktober 2011 obliegt dem Landesbeauftragten die Datenschutzaufsicht über nicht-öffentliche Stellen nach § 38 BDSG, § 22 Abs. 2 DSG LSA. Damit überwacht er nicht-öffentliche Stellen hinsichtlich der Ausführung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz (insofern über den Verbraucherdatenschutz hinausgehend), soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Daraus ergeben sich folgende *Einzelaufgaben*:

[1] http://www.marktwaechter.de

- Durchführung von anlassbezogenen und -unabhängigen Kontrollen, § 38 Abs. 1 Satz 1 BDSG,
- Beratung und Unterstützung der betrieblichen Beauftragten für den Datenschutz und der verantwortlichen Stellen, § 38 Abs. 1 Satz 2 BDSG,
- Fertigung eines Tätigkeitsberichts alle zwei Jahre, § 38 Abs. 1 Satz 7 BDSG,
- Registerführung meldepflichtiger automatisierter Verarbeitungen und Gewährung der Einsichtnahme für Jedermann, § 38 Abs. 2 BDSG,
- Prüfung der Verhaltensregeln von Berufsverbänden und anderer Vereinigungen, § 38a BDSG,
- Genehmigung von Datenübermittlungen in Drittstaaten, § 4c Abs. 2 BDSG.

Zur Wahrnehmung dieser Aufgaben hat der Landesbeauftragte nach pflichtgemäßem Ermessen folgende *Befugnisse*:

- Datenübermittlung an andere Aufsichtsbehörden, § 38 Abs. 1 Satz 4 BDSG,
- Unterrichtung des Betroffenen sowie Anzeige bei der für die Verfolgung und Ahndung zuständigen Stelle im Falle festgestellter Verstöße, § 38 Abs. 1 Satz 6 BDSG,
- Anzeige bei der Gewerbeaufsichtsbehörde im Falle schwerwiegender Verstöße, § 38 Abs. 1 Satz 6 BDSG,
- Auskunftsersuchen, § 38 Abs. 3 BDSG,
- Prüfungen bei den verantwortlichen Stellen während der Betriebs- und Geschäftszeiten, Einsichtnahme in geschäftliche Unterlagen, § 38 Abs. 4 BDSG,
- Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße, Verhängung von Zwangsgeldern zur Durchsetzung dieser Maßnahmen bis hin zur Untersagung des Einsatzes einzelner Verfahren, § 38 Abs. 5 Satz 1 und 2 BDSG,
- Aufforderung der Abberufung des betrieblichen Datenschutzbeauftragten bei fehlender Fachkunde und Zuverlässigkeit, § 38 Abs. 5 Satz 2 BDSG,
- Strafantragsrecht bei Straftaten nach dem BDSG, § 44 Abs. 2 BDSG.

Zum Auskunftsersuchen nach § 38 Abs. 3 BDSG ist eine Entscheidung des Verwaltungsgerichts Halle ergangen, welche die Auffassung des Landesbeauftragten bestätigt. Im Rahmen einer Anfechtungsklage gegen einen Auskunftsbescheid war streitig, ob der Landesbeauftragte eine verantwortliche Stelle befragen durfte, obwohl nicht mit Sicherheit feststand, dass die verantwortliche Stelle überhaupt personenbezogene Daten erhebt, verarbeitet oder nutzt. Nach dem Beschluss des Verwaltungsgerichts Halle vom 29. Juni 2015 (Az. 1 A 254/14 HAL) eröffnet § 38 Abs. 3 BDSG eine umfassende Auskunftspflicht der verantwortlichen Stellen. Die Vorschrift erfasst auch Auskunftsverlangen, die der Feststellung dienen, ob überhaupt eine Datenverarbeitung i. S. d. BDSG und damit die Zuständigkeit des Landesbeauftragten vorliegt.

Der Landesbeauftragte ist zudem gemäß § 22 DSG LSA zuständig für die Verfolgung und Ahndung datenschutzrelevanter *Ordnungswidrigkeiten*. Dies sind die Ordnungswidrigkeitstatbestände nach

- § 43 BDSG,
- § 16 Abs. 2 Nrn. 2 bis 5 TMG,
- § 111 Abs. 1 Nr. 1 SGB IV,
- § 85 SGB X,
- § 31a DSG LSA,

- § 130 Abs. 1 des Gesetzes über Ordnungswidrigkeiten, soweit die unterlassene Aufsichtsmaßnahme datenschutzrechtliche Zuwiderhandlungen gegen die eben genannten Vorschriften betrifft (seit 31. Juli 2015).

Aufgrund des vom Deutschen Bundestag am 17. Dezember 2015 beschlossenen Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts (BR-Drs. 4/16) wird dem Landesbeauftragten zusätzlich ein Anhörungsrecht im Rahmen verbraucherrechtlicher gerichtlicher Abmahnverfahren eingeräumt (vgl. § 12a des Unterlassungsklagengesetzes (UKlaG)).

Bereits im XI. Tätigkeitsbericht hat der Landesbeauftragte auf die nicht ganz einheitliche Rechtsprechung zur Frage der wettbewerbsrechtlichen Abmahnfähigkeit von Datenschutzverstößen durch sogenannte anspruchsberechtigte Stellen (insbesondere Verbraucherverbände) hingewiesen (Nr. 1.2). Nach bisheriger Rechtslage war lediglich eindeutig, dass die Abmahnung nach § 1 UKlaG erfolgen konnte, wenn die AGB, welche ein Unternehmer gegenüber Verbrauchern verwendet, gegen datenschutzrechtliche Vorschriften verstoßen. Bei einem anderweitigen Verstoß gegen Datenschutzrecht war aufgrund divergierender Entscheidungen der Gerichte nicht eindeutig geklärt, ob die anspruchsberechtigten Stellen im Wege einer Verbandsklage einen Unterlassungsanspruch nach § 2 Abs. 1 UKlaG geltend machen können. Ein solcher Anspruch besteht nur, wenn die konkret verletzten Datenschutzvorschriften als Verbraucherschutzgesetze anzusehen sind. Zivilgerichte haben dies aber überwiegend abgelehnt.

Erfreulich wäre aus Sicht des Datenschutzes, wenn alle Vorschriften, die für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Verbrauchers durch einen Unternehmer gelten, Verbraucherschutzgesetze im Sinne des § 2 Abs. 1 UKlaG wären und damit auch mithilfe der Verbandsklage durch die anspruchsberechtigten Stellen durchgesetzt werden könnten. So war es auch im ursprünglichen Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vorgesehen. Von einigen Aufsichtsbehörden – auch dem Landesbeauftragten – wurde darüber hinaus vorgeschlagen, dass Klagegrund auch Verstöße gegen technische und organisatorische Regelungen des Datenschutzes sein sollten. Zudem sollte zugunsten der Aufsichtsbehörden ein Anhörungsrecht implementiert werden, welches gewährleistet, dass der Sachverstand dieser Fachbehörden für die Gerichtsverfahren genutzt werden kann.

Bedauerlicherweise ist das jetzt beschlossene Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts hinter diesen Erwartungen zurück geblieben. Zwar wurde das Anhörungsrecht der Aufsichtsbehörden aufgenommen ebenso wie in § 2 Abs. 2 Nr. 11 UKlaG als Klagegrund die Verletzung von Vorschriften, die die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten regeln. Jedoch greift diese Vorschrift nur, wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden. Keine Möglichkeit der Verbandsklage besteht damit im weiten Bereich der Datenverarbeitung zu vertraglichen Zwecken.

Im XI. Tätigkeitsbericht (Nr. 3.1.3) hatte der Landesbeauftragte über die Entstehung der Stiftung Datenschutz und die Frage nach ihrer Unabhängigkeit berichtet. Zwischen dem Vorstand der Stiftung und dem Landesbeauftragten hat ein Austausch stattgefunden, in dem die Aktivitäten der Stiftung dargestellt wurden. Die Stiftung hat ihre Tätigkeit aufgenommen und auf ihrer Homepage Informationen zum Datenschutz (u. a. Praxistipps und Broschüren für Beschäftigte, Kinder und Jugendliche) angeboten.

1.3 Smarte Welten und Industrie 4.0

In seinem XI. Tätigkeitsbericht (Nr. 1.3) hatte sich der Landesbeauftragte mit dem Thema „Big Data“ kritisch auseinandergesetzt und entsprechende Forderungen zur Umsetzung des Datenschutzes bei Aus- und Verwertung von riesigen, oft unstrukturierten Datenmengen durch Unternehmen und Behörden formuliert. Im zurückliegenden Berichtszeitraum hat sich allerdings die umfassende Digitalisierung in Wirtschaft und Verwaltung sowie im privaten Lebensbereich weiter beschleunigt und durchdringt immer mehr die ganze Gesellschaft. So boomt z. B. auch der Einsatz von mobilen Endgeräten wie Smartphones und Tablets unbegrenzt weiter. Waren es laut Statistik im Jahr 2015 ca. 45 Millionen Smartphones in Deutschland, wird deren Anzahl im Jahr 2019 voraussichtlich bereits 55 Millionen betragen. Mobilität auch bei der Kommunikation, d. h. überall und jederzeit erreichbar sein, scheint gegenwärtig „das“ Gebot der Stunde zu sein.

Zeitgleich mit dem Boom der Nutzung von Smartphones bei der individuellen Kommunikation ist ein neuer Hype mit dem **Internet der Dinge** (engl. Internet of Things – IoT) zu verzeichnen. Wenn es nach der Einschätzung des Marktforschungsinstituts McKinsey geht, ist das IoT aber kein Hype, sondern ein sog. Business-Modell mit sehr viel wirtschaftlichem Potential. Die Experten prognostizieren der Weltwirtschaft einen Mehrwert von bis zu 1.100 Milliarden Dollar in den kommenden zehn Jahren.

Mit dem IoT soll die nächste große Innovationswelle im Rahmen der Digitalisierung von Wirtschaft und Gesellschaft einsetzen. Allgemein ist unter IoT die Vernetzung von Dingen mit Dingen – und zunehmend von Menschen mit Dingen – zu verstehen. Beispiele dafür sind sog. *Wearables*. Das sind direkt am Körper getragene Geräte oder auch Kleidungsstücke mit eingearbeiteter Sensorik und Computersystemen, die sich per App steuern und auswerten lassen. Zu den Wearables zählen z. B. auch Smartwatches, Fitness-Armbänder oder aber Steuerungs- und Messsensoren, die an verschiedenen Körperstellen (z. B. am Arm, am Gürtel oder um den Hals) befestigt werden können (Aktiv-Tracker) oder Brillen, deren Innenseiten als Bildschirm dienen (z. B. „Google Glass“). Dabei werden über unterschiedliche Sensoren Daten aufgezeichnet und diese dann direkt verarbeitet oder z. B. an Smartphones oder Laptops übertragen. Aber auch per App steuerbare Hauseinrichtungen beim Smart Home, das für die Vernetzung sowohl von Haustechnik als auch Haushaltsgeräten steht, oder selbstfahrende Autos (wie z. B. Google Driverless Car) zeigen an, in welche Richtung insbesondere die Entwicklung bei der Digitalisierung in Zukunft gehen wird. Ähnlich wie bei der industriellen Revolution im vorigen Jahrhundert dreht sich dabei alles um gesteigerte Effizienz, erhöhte Wertschöpfung und zusätzlichen Komfort. Durch die Verbindung und Vernetzung sowie die Vermischung von physischen und digitalen Welten soll ein erhebliches wirtschaftliches Potential für Konsumenten und Unternehmen bestehen.

Gegenwärtig bringt das IoT vorwiegend Neuerungen für Konsumenten. Das größte Potential besteht nach Expertenmeinung aber in sog. Business-Anwendungen für die **Industrie 4.0**. Die Digitalisierung und Vernetzung entlang dieser zukünftigen Wertschöpfungsketten wird dabei eng verknüpft mit zusätzlichem Nutzen von **Big Data**. IoT braucht Big Data. Nach Meinung des Markforschungsinstituts McKinsey werden gegenwärtig weniger als ein Prozent der vorhandenen Daten verwendet und dann meist nur zur Echtzeitüberwachung und Störungsanalyse eingesetzt. Da ohne den Einsatz leistungsfähiger Netzwerke, Komponenten und Datenverarbeitungssysteme IoT mehr Hype als Geschäftsmodell bleiben würde, ist mit einer weiteren Entwicklung entsprechender Anwendungsbeispiele durch marktführende Unternehmen der IT-Branche zu rechnen. Ein wesentlich größerer Mehrwert entsteht durch Optimierung und sinnvolle Vorausplanung bestehender Arbeitsabläufe. Dies hat allerdings auch Auswirkungen auf die Arbeitswelt insgesamt.

Das Gesundheitswesen (siehe Nr. 11.1.3, „Gläserner Patient“) und der Verkehrsbereich (siehe Nr. 16.3, „Gläserner Autofahrer“) sind Beispiele dafür, wie sich neben technischen Voraussetzungen auch die gesetzlichen Vorgaben wandeln müssen. Die Gewährleistung der Privatsphäre und des Datenschutzes, Schutz des geistigen Eigentums und Zuordnung der Datenhoheit sowie Verbesserungen der Informationssicherheit sind wichtigste Bedingungen und Voraussetzungen dafür, dass durch das IoT in naher Zukunft weitere Lebensbereiche erschlossen werden können.

Industrie 4.0 steht für die Entwicklung einer neuen Form der Industrialisierung. Nach Mechanisierung, Elektrifizierung und Informatisierung der Industrie erfolgt durch die immer weiter zunehmende Einbeziehung des Internets in Produktion und Fabrikation eine *vierte* industrielle Revolution. Unternehmen, auch aus verschiedenen Branchen, werden ihre Maschinen, Lagersysteme und Betriebsmittel weltweit miteinander vernetzen. Zukünftig werden sog. Smart Factories in der Lage seine, eigenständig Informationen auszutauschen, Aktionen auszulösen und einander gegenseitig zu steuern. Das Resultat sind intelligente (smarte) Produkte. Produkte sollen künftig in noch stärkerem Maße kontinuierlich Daten über ihren Zustand sammeln und selbständig übermitteln können. Die Informationen, die ein smartes Produkt im Laufe seines Lebens sammelt, können von den Herstellern direkt berücksichtigt werden und eine nahtlose Weiterentwicklung ermöglichen.

Mit dem Begriff „Smart Factory“ (intelligente Fabrik), einem Begriff aus der Forschung im Bereich Fertigungstechnik als Teil des Zukunftsthemas Industrie 4.0, wird dabei die Vision einer Produktionsumgebung, in der sich Fertigungsanlagen und Logistiksysteme *ohne* menschliche Eingriffe weitgehend selbst organisieren, bezeichnet. Technische Grundlage sind „Cyber-Physische Systeme“ (CPS; engl. cyber-physical system), welche mit Hilfe des IoT miteinander kommunizieren. Ein CPS bezeichnet den Verbund informations- und softwaretechnischer Komponenten mit mechanischen und elektronischen Teilen, die über eine Kommunikationsinfrastruktur, wie z. B. das Internet, kommunizieren. Damit steigt nicht nur die Menge der Daten, sondern vor allem auch deren Aussagekraft. Daten werden von smarten Maschinen autonom erzeugt und übermittelt. Sie überschreiten auch Unternehmensgrenzen. Durch diesen intensiven Datenaustausch bieten sich vielfältige Möglichkeiten zur Verknüpfung und zur Erstellung umfassender Persönlichkeitsprofile. Insbesondere durch die Zusammenführung von Daten mehrerer Unternehmen lassen sich Persönlichkeitsprofile zum Konsumverhalten erstellen, aus denen sich Rückschlüsse u. a. auf die finanziellen Verhältnisse der Kunden oder persönliche Lebensumstände ziehen lassen. Damit

besteht sicherlich ein erhebliches wirtschaftliches Interesse an der Kenntnis dieser Daten.

Durch die Smart Factory wird auch die zunehmende Berücksichtigung individueller Kundenwünsche möglich sein, zudem die Fähigkeit, individualisierte Einzelstücke rentabel zu produzieren. Die Individualisierung von Produkten wird sich nicht mehr auf Industriekunden, z. B. aus dem Anlagen- und Werkzeugmaschinenbau, und im Konsumgüterbereich auf Premiumprodukte beschränken. Es ist vielmehr davon auszugehen, dass sich die Berücksichtigung individueller Kundenwünsche bis auf alltäglich verwendete Produkte, wie z. B. Gebrauchsgegenstände, Kleidung oder Nahrungsmittel ausdehnen wird. Da intelligente Produktionsanlagen eine hohe Variantenanzahl der Produkte ermöglichen, können die Hersteller den individuellen Wünschen leicht nachkommen.

Die neuen Produktionsprozesse und Geschäftsnetzwerke in der Industrie 4.0 in Verbindung mit IoT und Big Data führen zu vielfältigen datenschutzrechtlichen Herausforderungen. Dies betrifft einerseits den Schutz der Unternehmensdaten, aber insbesondere auch den Schutz der personenbezogenen Daten von Kunden. Zwangsläufig geht die stark gestiegene Vernetzung, insbesondere die Einbindung der Kunden in den Gestaltungs- und Produktionsprozess, mit der Notwendigkeit eines intensiven und umfangreichen Datenaustauschs einher. Die Herstellung individualisierter Produkte führt zu einem intensiven Austausch mit Kunden und Geschäftspartnern. Intelligente (smarte) Objekte generieren zahlreiche Informationen, die über Firmengrenzen hinweg übermittelt werden. Um die übermittelten Daten vor Zugriffen Unbefugter zu schützen, muss einerseits eine komplexe Sicherheitsarchitektur entwickelt werden, andererseits muss es aber auch datenschutzrechtliche Vorgaben für den Umgang der Unternehmen mit den an sie übermittelten Kundendaten geben. Sollte sich die Vernetzung zwischen Unternehmen und Kunden zur Individualisierung von Produkten tatsächlich auf nahezu alle Bereiche des täglichen Lebens ausdehnen, führt dies auf Seiten der Unternehmen zu umfangreichen Datenbeständen zu den konsumierten Produkten und den damit verbundenen Kunden. Diese Datenbestände bergen erhebliche Missbrauchsgefahren.

Ein wichtiges Thema bei Industrie 4.0 wird Security by Design sein, d. h. die Berücksichtigung von Informationssicherheit und Datensicherheit bereits bei der Planung bzw. beim Entwurf von Smart Factories. Wesentlich wird auch eine Vertrauensinfrastruktur sein, um verlässliche Identitäten und die Systemintegrität entlang zukünftiger Wertschöpfungsketten zu gewährleisten. Grundlage könnte auch hier die kryptografisch basierte Ende-zu-Ende-Sicherheit sein. Dazu könnten u. a. auch Systeme gehören, welche die Integrität von CPS allerdings in Echtzeit prüfen und Angriffe automatisch erkennen und abwehren können. In industriellen Infrastrukturen werden zukünftig anders als gegenwärtig in der Unternehmens-IT Reaktionen in Echtzeit erfolgen müssen.

Die für diese zukünftige Entwicklung notwendigen datenschutzrechtlichen Regelungen und Schutznormen sind bisher noch nicht hinreichend bedacht worden. Deshalb ist es erforderlich, auch für den mit Industrie 4.0 beschriebenen Bereich datenschutzrechtliche Vorgaben zu erörtern und ggf. auszugestalten, auch wenn man hier erst am Beginn des Prozesses steht. Die entsprechenden Schutzvorkehrungen müssen mit der fortschreitenden technischen und technologischen Entwicklung Schritt halten. Die enorme Menge an gespeicherten Daten und deren hohe Aussagekraft und be-

sondere Sensibilität stellen zwar eine große Herausforderung für den datenschutzrechtlichen Regelungsrahmen dar. Dabei dürfte jedoch das vom Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 (NJW 2008, 322) entwickelte Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einen hilfreichen Ansatz bieten. Inwieweit die Europäische Datenschutz-Grundverordnung (vgl. Nr. 3.1.1) auf diesen technologischen Fortschritt ausreichende Antworten geben wird, bleibt abzuwarten. Notwendig ist grundsätzlich der angemessene Ausgleich zwischen ökonomischen Interessen der Unternehmen und dem Schutz der Persönlichkeitsrechte der Betroffenen. Der Landesbeauftragte wird diese Entwicklung weiterhin aufmerksam beobachten. Angesichts der Berechenbarkeit des Menschen durch Algorithmen und seiner dadurch möglichen Kontrolle durch Maschinen lauten einige der Grundfragen: Wo bleibt der Mensch? Wie gelingt freie Selbstbestimmung in der digitalen Gesellschaft?

Der Landtag und die Landesregierung von Sachsen-Anhalt haben sich mit dem Thema Industrie 4.0 bisher vornehmlich unter wirtschaftlichen Gesichtspunkten beschäftigt (siehe LT-Drs. 6/4243 und 6/4305 zu Ziffer 2). Datenschutzspezifische Ansätze sind noch nicht erkennbar.

1.4 Medienkompetenz

Aktivitäten hinsichtlich der Stärkung der Medienkompetenz und des Datenschutzbewusstseins im Bildungsbereich hatten für den Landesbeauftragten auch in diesem Berichtszeitraum einen hohen Stellenwert (vgl. XI. Tätigkeitsbericht, Nr. 9.5). Der Landesbeauftragte ist weiterhin Mitglied der Arbeitsgruppe „Medienbildung/Medienkompetenz“. Deren Hauptaufgabe ist die Begleitung der Umsetzung und Weiterentwicklung der Maßnahmen des „Konzeptes der Landesregierung für die Stärkung der Medienkompetenz in Sachsen-Anhalt“. Es gibt zwar kleine Erfolge, wo es gelungen ist, wichtige Projekte zu starten, wie z. B. die Einrichtung der (allerdings nur 11) medienpädagogischen Berater. Insgesamt ist der Schwung früherer Jahre jedoch verloren gegangen, insbesondere im Kultusministerium. Der geplante (Abschluss-)Bericht steht lange aus.

Die Implementierung des Themas Medien in die Erstausbildung der Lehrkräfte und die Einführung eines Pflichtfaches oder jedenfalls Pflichtkurses Medienkunde werden weiter diskutiert. Immerhin wurde in die Zielvereinbarungen 2015-2019 zwischen dem Ministerium für Wissenschaft und Wirtschaft und den Universitäten Magdeburg und Halle die Vorgabe aufgenommen, im Bereich der Bildungswissenschaften, einschließlich der Fachdidaktiken, verbindliche Inhalte zum systematischen Erwerb von Medienpädagogik und Medienkompetenz so zu verankern, dass sie einem in sich geschlossenen Konzept folgen und die Vermittlung als grundlegende und fachübergreifende Querschnittskompetenz gewährleisten. Damit wird auch einer Empfehlung des Landtages entsprochen (Beschluss vom 23. April 2015, LT-Drs. 6/4020, Nr. 1.a)).

Der Landesbeauftragte nahm die Beratungen der Landtagsausschüsse für Bundes- und Europaangelegenheiten sowie Medien und Bildung zum XI. Tätigkeitsbericht zum Anlass, zur allseits wachsenden Bedeutung der Vermittlung von Medienkompetenz näher auszuführen. Dabei stieß er auf breite Zustimmung hinsichtlich seiner Forderung nach mehr Verbindlichkeit, Nachhaltigkeit und Vernetzung der Konzepte,

Angebote und Maßnahmen für den schulischen und außerschulischen Bereich. Der Landtag griff dies in seinem Beschluss vom 5. Juni 2015 auf (LT-Drs. 6/4150, Nr. 3). Die Landesregierung lobt sich selbst mit ihren Hinweisen auf die medienpädagogischen Berater und Fortbildungsveranstaltungen für Lehrkräfte, übersieht dabei aber, dass es sich um freiwillige Angebote handelt, denen es an Verbindlichkeit fehlt (siehe Antwort der Landesregierung auf den vorerwähnten Landtagsbeschluss, LT-Drs. 6/4305, zu Nr. 3). Positiv hervorzuheben ist der Umstand, dass die Finanzierung der Netzwerkstelle Medienkompetenz bei der Landesmedienanstalt zunächst bis Ende 2016 gesichert ist. Die dritte Netzwerktagung Medienkompetenz Sachsen-Anhalt fand im September 2015 unter dem Titel „Medien/Familien/Interaktion - Herausforderungen zur Partizipation in der digitalen Gesellschaft“ statt und nahm den außerschulischen Bereich (z. B. Kindergärten, Familienleben, Freizeit) in den Blick; der Landesbeauftragte beteiligte sich erneut. Die Jugend- und Familienministerkonferenz hatte im Mai 2015 ein Eckpunktepapier „Aufwachsen mit digitalen Medien“ beschlossen und damit gerade für den außerschulischen Bereich die Bedeutung des Rechts aller Kinder und Jugendlichen auf ein gutes Aufwachsen mit Medien betont und als zentralen Umsetzungsaspekt einen modernen Jugendmedienschutz gefordert.

Die große Unterstützung seitens des Landtages für die Anliegen des Landesbeauftragten im Bereich der Medienkompetenzvermittlung stößt auf eine Diskrepanz zwischen Anspruch und Wirklichkeit: Denn die für die Geschäftsstelle des Landesbeauftragten für den Doppelhaushalt 2015/2016 beantragte Medienpädagogenstelle ist abgelehnt worden. Die Kapazitäten der Geschäftsstelle bleiben so begrenzt. Ein Medienpädagoge hätte Datenschutzthemen noch mehr in Fortbildungen, Workshops, Elternberatungen und Netzwerkarbeit einzubringen vermocht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat entschieden, die von Rheinland-Pfalz erstellte und betreute Datenschutzseite für Jugendliche **„www.youngdata.de“** als eine bundesweite Jugendseite aller Datenschutzbeauftragten zu übernehmen und weiterzuentwickeln. Dieses Angebot ist seit dem Safer Internet Day am 10. Februar 2015 online. Neben allgemeinen Informationen zum Datenschutz und speziellen Hinweisen z. B. zu Facebook, WhatsApp, Google, Cybermobbing und Videoüberwachung, stellen die jeweiligen Datenschutzbeauftragten unter „Bildungsangebote in deiner Region“ eigene landesspezifische Informationen bereit.

Die Bedeutung digitaler Bildung und entsprechende Forderungen nach mehr Aktivitäten wachsen stetig an. Dies belegen nicht nur die im XI. Tätigkeitsbericht (Nr. 9.5) erwähnten Empfehlungen etwa auch der Kultusministerkonferenz, sondern auch wissenschaftliche Studien, wie etwa die Internationale Bildungsstudie ICILS 2013 (International Computer and Information Literacy Study zu Computerkenntnissen von Achtklässlern), sondern auch weitere Vorstöße auf Bundes- und Länderebene. Beispielhaft sei auf die Positionspapiere der Netzwerke „Keine Bildung ohne Medien“ und „Initiative D21“ und den vom Deutschen Bundestag am 2. Juli 2015 beschlossenen Antrag der Fraktionen der CDU/CSU und SPD zur Stärkung der Medienkompetenz der Bürgerinnen und Bürger unter Einbeziehung von Fragen des Datenschutzes und der Datensicherheit (BT-Drs. 18/4422 und 18/5368) hingewiesen. Auf Bundesebene, etwa auch in der Digitalen Agenda 2014-2017 der Bundesregierung, wird stärker auch auf eine Förderung der MINT-Fächer und dabei insbesondere auf einen zeitgemäßen Informatikunterricht ab der Grundschule Wert gelegt. Der Bund will mit den Ländern eine „Strategie Digitales Lernen“ entwickeln.

Die Internetnutzung gehört zum Alltag von Kindern und Jugendlichen. Dies belegen etwa die Milieustudien des Deutschen Instituts für Vertrauen und Sicherheit im Internet.

Im September 2015 zog eine gemeinsame Arbeitstagung der Gemischten Kommission der Kultusministerkonferenz und der Länderkonferenz Medienbildung eine Zwischenbilanz des erreichten Standes und der bestehenden Defizite drei Jahre nach der Erklärung jener Konferenz zur Medienbildung in der Schule. Die Kultusministerkonferenz verabschiedete im Oktober 2015 einen Verfahrensvorschlag zur Entwicklung einer Strategie „Bildung in der digitalen Welt“, die 1. Bildungspläne aller Fächer, 2. Aus-, Fort- und Weiterbildung von Erziehenden und Lehrenden, 3. IT-Infrastruktur und Ausstattung, 4. Bildungsmedien, 5. E-Government-Module und IT-Managementsysteme und 6. rechtliche Rahmenbedingungen als Handlungsfelder erfassen soll. Der zuständige Arbeitskreis der Datenschutzkonferenz soll noch in die Beratungen einbezogen werden.

Im Grunde verdienen die vorgenannten inhaltlichen Aspekte und Handlungsfelder einen eigenen Tätigkeitsbericht. Der Landesbeauftragte kann die Themenstellungen letztlich hier nur kursorisch darstellen.

Im Frühjahr und Sommer 2015 begann eine politische Debatte über die zunächst insbesondere vom Ministerium der Finanzen mittels eines „Letter of Intent“ angestrebte *Bildungspartnerschaft* mit der Firma Microsoft Deutschland GmbH. Inhaltlich betrifft diese die Schaffung der notwendigen IT-Infrastruktur über das STARK III-Programm der Europäischen Kommission und die Ausstattung der Schulen mit Anwendungssoftware (Microsoft Office). Weiterhin umfasst die Bildungspartnerschaft die Zurverfügungstellung einer Plattform mittels Cloud-Lösung und die Einrichtung einer IT-Akademie für die Lehrerfortbildung. Das Vorhaben soll sich in die Strategie Sachsen-Anhalt digital 2020 einordnen. Ein Konzept „Lernen, Lehren, Managen 2.0 – auf dem Weg zur Schule 2020“ (mit Aussagen zur Bedeutung von IKT im Bereich von Infrastruktur, Pädagogik und Bildungsmanagement) wurde im Frühherbst übersandt; es enthält aber keine Hinweise zur Bildungspartnerschaft. Das Projekt der Bildungspartnerschaft mit Microsoft wurde dem Landesbeauftragten aus Presseberichten bekannt. Seine Nachfragen bei Finanz- und Kultusministerium ergaben erst im Spätherbst substanzielle Aussagen und Antworten.

Der Landesbeauftragte betrachtete das Projekt skeptisch vor dem Hintergrund der Datenschutzanforderungen bei ausländischen Cloud-Lösungen (vgl. auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. September und 1. Oktober 2015, **Anlage 33**) und angesichts des ungeklärten Verhältnisses zu vorhandenen Lernplattformen (siehe Nr. 9.2.3). Er ist der Überzeugung, dass Technikausstattung zwecks Förderung digitaler Kompetenz nicht ohne ein ganzheitliches Bildungskonzept mit den Komponenten Medienkompetenz und Datenschutz umgesetzt werden sollte. Der Landtag gab die Prämisse vor, dass keine personenbezogenen Daten zu Microsoft fließen dürfen (LT-Drs. 6/4491). In den Erörterungen mit Finanz- und Kultusministerium wurde bekannt, dass Microsoft eine deutsche Cloud-Lösung (Treuhänder-Modell) anstrebt. Ob und inwieweit dadurch datenschutzrechtliche Bedenken ausgeräumt werden können, blieb noch offen. Dies gilt zumal in Bezug auf die Nutzung von Microsoft Office 365 Pro Plus im Zusammenhang mit der geplanten anonymen Anmeldung eines jeden Schülers und Lehrers

für ein Microsoft-Konto (Anmeldung in einer Cloud) zur privaten Nutzung durch Schüler und Lehrer.

Wenn es dem Kultusministerium nur um die einheitliche Ausstattung aller Schulen des Landes mit Microsoft Office-Software gegangen wäre, hätte die Beschaffung über einen landesweiten EES-Rahmenvertrag (sog. Volumenlizenzvertrag – Enrollment for Education Solution) für den Bereich Forschung und Lehre auf der Basis der Anzahl von Vollzeitmitarbeitern (hier: Lehrer und Schüler) erfolgen können, *ohne* Erhebung personenbezogener Daten.

Ein Beispiel für eine solche datenschutzgerechte Vorgehensweise ist das im Salzlandkreis verwirklichte Pilotprojekt „IT macht Schule“. Der Landesbeauftragte hat im zurückliegenden Berichtszeitraum dieses Projekt beratend begleitet. Leider haben sich bisher weder das Ministerium der Finanzen noch das Kultusministerium umfassend inhaltlich mit diesem Konzept und dem Projekt als Alternative zum nunmehr eingeschlagenen Weg der Bildungspartnerschaft mit Microsoft beschäftigt bzw. auseinandergesetzt.

Mit diesem Projekt im Salzlandkreis wird noch eine weitere Herausforderung deutlich: Nicht alle Schulträger bzw. Schulen werden sich an der Bildungspartnerschaft mit Microsoft beteiligen. Doch auch für diese Schulen bedarf es der Einführung und Umsetzung von Konzepten zum digitalen Lernen.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die **Geschäftseingänge** entwickelten sich wie folgt:

2013: 4.742 2014: 5.163 2015: 5.230

Für diese Zeiträume gab es insgesamt 230 Petenteneingaben im Bereich des Datenschutzes bei öffentlichen Stellen, im Einzelnen:

2013: 90 2014: 66 2015: 74

Im Bereich des Datenschutzes im nicht-öffentlichen Bereich fielen folgende Fallzahlen bei den Eingaben an:

2013: 95 2014: 120 2015: 142

Zu den vorgenannten Zahlen kamen viele Behörden- und Firmenanfragen hinzu. Die Mitarbeiter und Mitarbeiterinnen der Geschäftsstelle des Landesbeauftragten nahmen zahlreiche **Informationsbesuche und Beratungsgespräche** wahr. In den vorgenannten Zeiträumen wurden insgesamt 15 Ordnungswidrigkeitsverfahren eingeleitet.

Kontrollen bei öffentlichen wie nicht-öffentlichen Stellen erfolgten überwiegend anlassabhängig. Trotz der hohen Arbeitsbelastungen gelang es aber in den vergangenen Jahren, auch wieder **anlassunabhängige Kontrollen** durchzuführen. Schwerpunkte waren u. a. Querschnittsprüfungen in vier Kommunen, die Kontrolle von zwei

Krankenhäusern, die Prüfung einer Krankenkasse im Krankengeldfallmanagement, dreier Gymnasien und einer integrierten Gesamtschule. Des Weiteren wurden vier Personalämter, ein Fundbüro, eine Ausländerbehörde, ein Finanzamt, ein Jobcenter, ein Sozialamt und vier Ministerien in Bezug auf Sicherheitsakten im Geheimschutz kontrolliert. Zusätzliche Prüfungsschwerpunkte waren Webshops von Apotheken und Videoüberwachungen in Bäckereien.

Die **Öffentlichkeitsarbeit** umfasste neben der Homepage der Behörde die Pressearbeit sowie die Herausgabe von Broschüren und weiterem Informationsmaterial.

Der Landesbeauftragte hatte am Tag der offenen Tür des Landtags von Sachsen-Anhalt am 3. Oktober 2014 Gelegenheit, seine Behörde mit einem eigenen Stand im Landtagsgebäude vorzustellen. So ergab sich die Möglichkeit, das Angebotsspektrum des Landesbeauftragten an Broschüren, Informationsheften und Faltblättern zum Datenschutz und auch zur Informationsfreiheit den vielen interessierten Besuchern auszuhändigen. Nachfragen machten das Interesse an den Themen besonders deutlich.

Die Zusammenarbeit mit dem Landtagspräsidenten und seiner Landtagsverwaltung erfolgte im Übrigen weiter vertrauensvoll und konstruktiv.

Da die Struktur der Wirtschaft in Sachsen-Anhalt weitgehend nicht von großen international aufgestellten Unternehmen bestimmt wird, sondern flächendeckend von vielen kleinen und mittleren Unternehmen, hat der Landesbeauftragte speziell für diese Zielgruppe eine Broschüre unter dem Titel *„Datenschutz ist Chefsache“* herausgegeben. Auch die Kunden von Unternehmen, speziell die Verbraucher, wurden nicht außer Acht gelassen. In Zusammenarbeit mit der Verbraucherzentrale Sachsen-Anhalt wurde ein Faltblatt mit dem Titel *„Datenschutz – Kennen Sie Ihre Rechte als Verbraucher?“* veröffentlicht.

Auch wurden **Fortbildungen** für Behördenbedienstete des Landes im Rahmen des Programms des Aus- und Fortbildungsinstituts Sachsen-Anhalt angeboten.

Der Landesbeauftragte und einzelne Mitarbeiter hielten bei verschiedenen Gastgebern Vorträge zur Entwicklung des Datenschutzes und zu spezifischen Fachthemen. Auch wurden Beiträge in Mitglieder- und Fachzeitschriften veröffentlicht.

Die Pflege und Wahrnehmung der **Datenschutznetzwerke** wurde fortgesetzt. So wurden Erfahrungsaustausche mit den behördlichen Datenschutzbeauftragten der Hochschulen des Landes ebenso durchgeführt wie solche jährlichen Gesprächsrunden mit den behördlichen Datenschutzbeauftragten der Landkreise und kreisfreien Städte. Diese Treffen haben sich als wichtiger Netzwerkbaustein fest etabliert; neben Erörterungen zu allgemeinen datenschutzrechtlichen Entwicklungen geht es immer wieder um Berichte und Fragestellungen aus der Praxis zu Aspekten des Datenschutzes und der Datensicherheit.

Der Landesbeauftragte beteiligte sich weiterhin am Erfahrungsaustauschkreis Sachsen-Anhalt der Gesellschaft für Datenschutz und Datensicherheit e. V. für betriebliche Datenschutzbeauftragte und an Informationsveranstaltungen von Kammern und Verbänden für Unternehmensvertreter. Dieser Adressatenkreis wird ab dem Jahr

2016 im Hinblick auf die Änderungen im Datenschutzrecht durch die Europäische Datenschutz-Grundverordnung in besonderer Weise im Mittelpunkt stehen.

Das aktuelle *Organigramm der Geschäftsstelle* ist beigefügt (**Anlage 47**). Durch die erheblichen Aufgabenzuwächse in der Übergangsphase bis zum Inkrafttreten der Europäischen Datenschutz-Grundverordnung und die auf den Landesbeauftragten und seine Geschäftsstelle zukommenden zusätzlichen Befugnisse ist ein deutlicher Stellenzuwachs erforderlich. Für den Doppelhaushalt 2015/16 wurde nur eine Referentenstelle im Bereich des nicht-öffentlichen Datenschutzes bewilligt. Eine zusätzlich angemeldete Juristenstelle für die Bereiche E-Government und Innere Sicherheit auch vor dem Hintergrund europäischer Entwicklungen wurde abgelehnt. Der Landesbeauftragte ist in den vergangenen Jahren nicht in der Lage gewesen, den Herausforderungen der Entwicklungen im Datenschutz und den daraus resultierenden Aufgabenstellungen in jeder Weise gerecht zu werden. Für eine unabhängige und effektive Tätigkeit zum Schutz der informationellen Selbstbestimmung der Menschen reicht die bisherige insbesondere personelle Ausstattung nicht aus. Dies gilt auch für die Aufgaben auf dem Feld der Medienkompetenzvermittlung (vgl. Nr. 1.4).

Die Zusammenarbeit auf der Ebene der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** bzw. der unabhängigen Datenschutzaufsichtsbehörden und in ihren Arbeitskreisen und Arbeitsgruppen für den Datenschutz im öffentlichen und nicht-öffentlichen Bereich ist in den letzten Jahren noch intensiver geworden und für die eigene Arbeit unentbehrlich.

2.2 Schwerpunkte und Empfehlungen

Im Folgenden werden im Sinne eines zusammenfassenden Rückblicks und Ausblicks wesentliche Schwerpunkte der Tätigkeit des Landesbeauftragten aufgeführt.

Wichtige Einzelfälle im Berichtszeitraum und zugleich längerfristige Vorgänge:

- Europäische Datenschutz-Grundverordnung (siehe Nr. 3.1.1)
- Safe Harbor (siehe Nr. 3.2.1)
- Datenschutzgesetz Sachsen-Anhalt (siehe Nr. 3.1.3)
- E-Government-Gesetzgebung (siehe Nr. 4.3)
- Dataport (siehe Nr. 4.6)
- Nutzung sozialer Netzwerke (siehe Nr. 5.8.1)
- Entwicklung des Verfassungsschutzes (siehe Kapitel 8)
- Landeskrebsregister (siehe Nr. 11.1.9)
- Videoüberwachung (siehe Kapitel 15)
- Medienkompetenzvermittlung (siehe Nr. 1.4)

Der Landesbeauftragte beteiligte sich beratend an folgenden wesentlichen Gesetzgebungsvorhaben:

- Europäische Datenschutz-Grundverordnung (siehe Nr. 3.1.1)
- Datenschutzgesetz Sachsen-Anhalt (siehe Nr. 3.1.3)
- Ausführungsrecht des Landes zum Bundesmeldegesetz (siehe Nr. 6.5.2)
- Weiterentwicklung des Justizvollzuges in Sachsen-Anhalt (siehe Nr. 7.2)
- Archivrechtsnovelle (siehe Nr. 10.1)
- Kommunalverfassungsgesetz (siehe Nr. 13.4.1)
- Gaststättengesetz (siehe Nr. 14.7)

Ungeachtet der Empfehlungen und Forderungen in den Einzelbeiträgen äußert der Landesbeauftragte folgende *Grunderwartungen gegenüber Landtag und Landesregierung für die 7. Wahlperiode*:

- Anpassung der Personal- und Sachausstattung der Geschäftsstelle des Landesbeauftragten an die neuen Aufgaben und Befugnisse aus der Europäischen Datenschutz-Grundverordnung
- Stärkere Berücksichtigung der Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
- Beteiligung des Landesbeauftragten bei der Entwicklung und Umsetzung einer Digitalen Agenda des Landes
- Umsetzung der Vorschläge der Enquete-Kommission des Landtages der 6. Wahlperiode für die Themenbereiche E-Government und Open Government
- Schaffung einer sicheren Kommunikation als Voraussetzung für ein vertrauenswürdiges E-Government
- Grundrechtskonforme Reform der Sicherheitsgesetze
- Intensivierung der Umsetzung der Konzepte zur Medienkompetenzbildung

Der Landesbeauftragte sieht für die kommenden Jahre folgende Bereiche als besondere Herausforderungen und Aufgabenfelder für den Datenschutz:

- Umsetzung und Anwendung der Europäischen Datenschutz-Grundverordnung
- Digitale Gesellschaft (Big Data, Internet der Dinge, Industrie 4.0)
- E-Government

- Innere Sicherheit
- Bildung/Medienkompetenz

3 Nationales und internationales Datenschutzrecht

3.1 Novellierung des Datenschutzrechts

Mit der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 „Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!“ (**Anlage 3**) machten die Datenschutzbeauftragten darauf aufmerksam, dass in vielen gesellschaftlichen Bereichen durch verfassungskonforme Regelungen auf fehlenden Grundrechtsschutz dringend zu reagieren sei. Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Gesetzliche Schutzvorkehrungen und Maßnahmen sind daher u. a. geboten im eingriffsintensiven Bereich der öffentlichen Sicherheit (vgl. Nr. 8.1, **Anlage 1**), im Sozial- und Gesundheitswesen (vgl. Nr. 11.1, **Anlage 4**) und bezüglich der Vertraulichkeit und Integrität elektronischer Kommunikation (vgl. Nr. 5.1, **Anlage 5**).

3.1.1 Datenschutz-Grundverordnung

Im XI. Tätigkeitsbericht (Nr. 3.1.1) berichtete der Landesbeauftragte von den Bestrebungen zur Verabschiedung einer *Europäischen Datenschutz-Grundverordnung*.

Die endgültige Verabschiedung der Datenschutz-Grundverordnung gemeinsam mit der Richtlinie zum Schutz personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr soll voraussichtlich noch im ersten Quartal 2016 erfolgen. Das Trilogverfahren, in welchem sich Europäisches Parlament, Ministerrat und Europäische Kommission auf gemeinsame Formulierungen einigten, fand im Dezember 2015 seinen Abschluss. Somit werden beide Regelungen voraussichtlich ab Mitte 2018 zur Anwendung kommen.

Jeder Kompromiss, der in den Verhandlungen über eine Fassung der Grundverordnung erörtert wurde, beinhaltete die Gefahr, dass dabei zentrale Datenschutzgrundsätze ausgehebelt werden. Aus diesem Grunde hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 18. und 19. März 2015 auf wichtige Punkte hingewiesen und insbesondere Positionen des Ministerrates kritisiert (**Anlage 28**). Einige Kritikpunkte finden sich auch in Beschlüssen des Bundesrates vom 28. November 2014 und 10. Juli 2015 (BR-Drs. 550/14 und 290/15).

Nachdem über 5000 Änderungswünsche für die Datenschutz-Grundverordnung gesichtet und bewertet wurden, konnten die Fassungen des Rates, der Kommission und des Parlamentes für eine Datenschutz-Grundverordnung nebeneinander in den sogenannten Trilogverhandlungen diskutiert werden. Im Wissen um diese entscheidende Phase der Entstehung der Datenschutz-Grundverordnung haben sich die Datenschutzbeauftragten des Bundes und der Länder am 14. August 2015 nochmals auf ein Kernpunktepapier verständigt (**Anlage 31**).

Wesentliche materielle Inhalte der neuen Datenschutz-Grundverordnung betreffen die Regelung des „Rechts auf Vergessenwerden“, das Recht auf Datenportabilität, Regelungen zu „Privacy by Design, Privacy by Default“ und eine Verschärfung der Bußgeldvorschriften.

Die Datenschutz-Grundverordnung ersetzt als unmittelbar geltendes Recht voraussichtlich ab Mitte 2018 sowohl das BDSG (nicht-öffentlicher Bereich und Bundesbehörden) und das DSG LSA (öffentlicher Bereich des Landes). Lediglich in Teilbereichen werden für den nationalen Gesetzgeber Öffnungsklauseln eingeräumt. Mit der Schaffung von neuen Rechtsgrundlagen, die mittels der Datenschutz-Grundverordnung dann einheitlich in ganz Europa gelten sollen, verändert sie auch Umfang und Qualität der Arbeit der Datenschutzaufsichtsbehörden und somit des Landesbeauftragten erheblich.

Der Landesbeauftragte ist gegenwärtig Aufsichtsbehörde für den nicht-öffentlichen Bereich (Wirtschaft, Freie Berufe, Privatpersonen etc.). Hinsichtlich des öffentlichen Bereichs ist er bislang Beschwerde- und Eingabestelle. Nach der Reform wird der Landesbeauftragte auch in diesem Bereich rechtlich als *Aufsichtsbehörde* gegenüber sämtlichen öffentlichen Stellen des Landes tätig sein. Dies schließt auch die Ministerien und die Landtagsverwaltung mit ein.

Gleichzeitig wird das bisherige Beanstandungsrecht im öffentlichen Bereich abgelöst von einer gerichtlich überprüfbaren *Anweisungs- und Anordnungsbefugnis*. Schon alleine diese Veränderung der Aufgaben und Befugnisse im öffentlichen Bereich wird zu erheblichen rechtlichen wie praktischen Verpflichtungen führen, die einen entsprechenden Personalaufwuchs zwingend erforderlich machen.

Für den Gesamtbereich des Datenschutzes werden folgende Aufgaben und wesentliche Erweiterungen durch die Datenschutz-Grundverordnung geregelt:

- Sofern Unternehmen keine Niederlassung in der EU haben, müssen sie wegen des *Marktortprinzips* die Datenschutz-Grundverordnung anwenden. Damit ist die Aufsichtsbehörde zukünftig die *Anlaufstelle* für sämtliche Fragen im Zusammenhang mit der Einhaltung der Datenschutz-Grundverordnung im Rahmen der Tätigkeit dieser Unternehmen.

- *Datenschutz-Folgeabschätzung*: Die Aufsichtsbehörde erstellt eine Liste von Verarbeitungsvorgängen, für die Datenschutz-Folgeabschätzungen durchzuführen sind. Diese veröffentlicht und übermittelt sie an den Europäischen Datenschutzausschuss oder gibt alternativ eine Negativliste heraus. Soweit ein grenzüberschreitender Bezug festgestellt wird, ist das europäische Kohärenzverfahren vor der Erstellung der Liste durchzuführen.

- *Vorherige Konsultation*: Der Verantwortliche muss vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate ziehen, wenn sich aus der Datenschutz-Folgeabschätzung ein hohes Risiko ergibt und der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Die Aufsichtsbehörde hat grundsätzlich nach *sechs Wochen* (!) eine schriftliche Empfehlung zu geben, wenn sie der Auffassung ist, dass die geplante Datenverarbeitung nicht mit der Datenschutz-Grundverordnung in Übereinklang steht.

- Die Neuregelung führt zu erweiterter Zusammenarbeit des betrieblichen bzw. behördlichen Datenschutzbeauftragten mit der Aufsichtsbehörde.

- Genehmigung von *Verhaltensregeln* zur ordnungsgemäßen Anwendung der Verordnung und deren Überwachung einschließlich der Akkreditierung geeigneter Stellen und Abstimmung im Kohärenzverfahren.

- Zukünftig wird der Landesbeauftragte Zertifizierungskriterien genehmigen und auch *Zertifizierungen* durchführen. Dies beinhaltet auch die regelmäßige Überprüfung der Zertifizierungen. Des Weiteren verpflichtet die Datenschutz-Grundverordnung die Aufsichtsbehörde dazu, die Einführung von Datenschutzzertifizierungen, -siegeln und -prüfzeichen anzuregen.

- Verbindliche *unternehmensinterne Datenschutzvorschriften*: Der Landesbeauftragte wird zukünftig entsprechende Datenschutzvorschriften genehmigen und ggf. auch das Kohärenzverfahren europaweit durchführen.

- Der Landesbeauftragte kann als Aufsichtsbehörde *Standardvertragsklauseln* (z. B. für die Auftragsdatenverarbeitung) im europäischen Kohärenzverfahren festlegen.

- Regelung der *Aufklärungsverpflichtung* der Aufsichtsbehörde. Hierunter fallen Sensibilisierungs- und Aufklärungspflichten gegenüber der Öffentlichkeit und in besonderer Weise gegenüber Kindern, die Aufklärung der für die Verarbeitung Verantwortlichen und der Auftragsdatenverarbeiter über deren Pflichten und schließlich die Information von betroffenen Personen über die Ausübung ihrer Rechte.

- Die *Abhilfebefugnisse* werden erweitert. Erstmalig ist auch für den öffentlichen Bereich der Erlass von Anordnungen geregelt, um die Datenverarbeitung mit der Datenschutz-Grundverordnung in Einklang zu bringen.

- Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden (*One-Stop-Shop*): Formale Regelung der europaweiten Abstimmungs- und Kooperationsverpflichtung mit engem Zeitfenster (vier Wochen), die zu einem erheblichen Mehraufwand führen wird.

- Verpflichtung zur gegenseitigen *europaweiten Amtshilfe*: Spätestens innerhalb *eines Monats* (!) nach Eingang des Ersuchens ist die Aufsichtsbehörde verpflichtet zu handeln.

- *Kohärenzverfahren* und Beteiligung beim *Europäischen Datenschutzausschuss*: Im Rahmen des Kohärenzverfahrens sollen europaweit abgestimmte einheitliche rechtliche Bewertungen und praktische Verfahrensweisen beschlossen werden. Auch hier sind kurze Fristen von einem Monat zu beachten.

- Es wird die *internationale Amtshilfe* als neue Verpflichtung ausdrücklich geregelt.

Es bleibt abzuwarten, inwieweit der nationale Gesetzgeber den ihm eingeräumten Spielraum für verbleibendes nationales Datenschutzrecht (z. B. Beschäftigtendatenschutz) nutzen wird. Die Anwendung der Datenschutz-Grundverordnung kann zu einer erheblichen Unsicherheit bei der Auslegung des Datenschutzrechts führen. Zum einen sind Teile der Verordnung nicht so ausführlich ausgestaltet wie das bisherige nationale Datenschutzrecht. Zum anderen sind die bisherigen Regelungen, Arbeitshilfen, Orientierungshilfen und Urteile nicht oder nur eingeschränkt verwendbar, weil sich die zugrunde liegenden Normen mit der Abschaffung der nationalen Regelungen verändern werden. Der Landesbeauftragte wird sowohl die Umstellung des Datenschutzrechts als auch die Anpassung der Landesgesetze an die neuen europäischen Vorgaben aktiv begleiten müssen.

Neben der Datenschutz-Grundverordnung tritt auch noch die *Richtlinie zum Schutz personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr* in Kraft. Diese enthält vor allem Regelungen für Polizei und Teile der Justiz. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder kommentierte auch diesen Textentwurf kritisch (siehe **Anlage 34**). Jedoch wurde der Anwendungsbereich der Richtlinie infolge eines weiten Begriffs der Gefahrenabwehr zulasten der Datenschutz-Grundverordnung ausgeweitet. Im Unterschied zu einer europäischen Verordnung ist bei einer europäischen Richtlinie die Umsetzung durch den nationalen bzw. Landesgesetzgeber weiterhin erforderlich. Der Landesbeauftragte wird die Formulierung der Umsetzungsgesetze auch in diesem Bereich aktiv unterstützen.

3.1.2 Beschäftigtendatenschutz

Im XI. Tätigkeitsbericht (Nr. 3.1.2) hatte der Landesbeauftragte über die Bemühungen berichtet, auf dem Gebiet des Beschäftigtendatenschutzes zu einer umfassenden gesetzlichen Regelung zu gelangen. Bisher ist es jedoch bei der Ausgestaltung des § 32 BDSG geblieben, sodass weiterhin nur aus der vielfältigen Rechtsprechung Erkenntnisse über die Rechtslagen im Beschäftigtendatenschutz zu gewinnen sind. Insoweit steht der Landesbeauftragte im Austausch mit den anderen Aufsichtsbehörden, beobachtet die Rechtsprechung und berät die öffentlichen und nicht-öffentlichen Stellen, u. a. in Einzelfällen und durch Broschüren oder Vorträge. Auch erging die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 „Beschäftigtendatenschutzgesetz jetzt!“ (**Anlage 9**). Es müssen dringend gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten sicherzustellen. Die Europäische Datenschutz-Grundverordnung bekräftigt mit einer Öffnungsklausel für den Regelungsbereich des Beschäftigtendatenschutzes den Handlungsbedarf auf mitgliedstaatlicher Ebene.

3.1.3 DSG LSA

Auf die Erarbeitung eines Entwurfs eines Gesetzes zur Dritten Änderung datenschutzrechtlicher Vorschriften und die vorausgehenden Beschlüsse des Landtages ist der Landesbeauftragte bereits im XI. Tätigkeitsbericht (Nr. 3.1.5) eingegangen. Bei den dort beschriebenen Verbesserungen im Detail ist es im Wesentlichen geblie-

ben. Lediglich die zunächst angedachte Regelung, die auf die Verschlüsselung im Zusammenhang mit „Cloud Computing“ abzielte, rief im Laufe der Beratungen des Gesetzentwurfs im Landtag Bedenken hervor, denen sich der Landesbeauftragte letztlich anschloss. Auftraggeber von Datenverarbeitungen bedienen sich gelegentlich auch sogenannter Public Clouds, die, wie bekannt geworden war, teilweise unbefugten Zugriffen unterlagen. Die grundsätzlich in die richtige Richtung zielende Regelung hätte ggf. doch keinen hinreichenden Datenschutz gebracht.

Das geänderte Datenschutzgesetz Sachsen-Anhalt vom 21. Juli 2015 (GVBl. LSA S. 365) ist Teil der Bekanntmachung der Neufassung vom 13. Januar 2016 (GVBl. LSA S. 24).

Einen besonderen Aspekt des Gesetzgebungsverfahrens stellten die optisch-elektronischen Einrichtungen zur Wildbeobachtung dar (sogenannte Wildkameras). Es sollte eine Regelung für Behörden getroffen werden (zu Wildkameras im nicht-öffentlichen Bereich hatte sich der Landesbeauftragte im XI. Tätigkeitsbericht, Nr. 4.17.6, ausführlich geäußert; siehe auch unten Nr. 15.2.13). Ihre Aufstellung soll insbesondere Erkenntnissen zur Verbreitung des Luchses im Harz und die Auswirkung auf Bestände anderer Wildarten dienen. Hierzu war zunächst eine Aufnahme einer Regelung in das DSG LSA angedacht. Der Landesbeauftragte hat sich gegen diesen Regelungsort ausgesprochen. Abschließend wurde eine Regelung in das Landesjagdgesetz aufgenommen.

Durch Wildkameras können nicht nur Tiere, sondern auch Menschen aufgenommen werden. Art und Zeit der Nutzung von Wald und Flur werden so gegebenenfalls personenbezogen bzw. personenbeziehbar festgehalten; auch ist das Recht am eigenen Bild betroffen. Deshalb hat der Landesbeauftragte Vorschläge zu einschränkender sachdienlicher Bestimmtheit der gesetzlichen Voraussetzungen gemacht. Weiter hat er sich für eine Angleichung an die Regelungen des DSG LSA zu optisch-elektronischer Beobachtung ausgesprochen. Damit sollte sichergestellt werden, dass dort, wo mit dem Aufenthalt von Personen im Aufnahmebereich zu rechnen ist, das Aufstellen einer solchen Kamera von vornherein ausgeschlossen ist. Im Übrigen ist vorgesehen, für den dann wohl äußerst seltenen Fall der Aufnahme eines Menschen diese sofort zu löschen. Die Vorschläge fanden Eingang in den Gesetzestext (Gesetz vom 21. Juli 2015, GVBl. LSA S. 365, 368).

Ein weiterer Schwerpunkt der Erörterungen im Gesetzgebungsverfahren war der Aspekt der europarechtlich vorgegebenen Unabhängigkeit des Landesbeauftragten. Die Unabhängigkeitsfrage gewann Bedeutung angesichts einer Änderung des Bundesdatenschutzgesetzes, die aufgrund europarechtlichen Anpassungsbedarfs erfolgte. Dazu erging die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 „Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar“ (**Anlage 17**). Mit dem Zweiten Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 25. Februar 2015 (BGBl. I S. 162) wurde die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als oberste Bundesbehörde eingerichtet und ausgestattet.

Vor diesem Hintergrund wies der Landesbeauftragte abermals darauf hin, dass im Hinblick auf seine Personalkompetenzen aufgrund der gesetzlichen Gesamtsituation in Sachsen-Anhalt Zweifel bestehen. Die Gefährdung der völligen Unabhängigkeit der Datenschutzaufsicht infolge denkbarer Einwirkungen im Personalbereich war

Gegenstand einer Entscheidung des EuGH vom 16. Oktober 2012 (Az. C-614/10). Ein weiterer wesentlicher Aspekt der Unabhängigkeit betrifft die finanzielle und personelle Ausstattung des Landesbeauftragten (vgl. **Anlage 41**). Da der Landesbeauftragte nicht als oberste Landesbehörde eingerichtet ist, kann das Verfahren zur Haushaltsanmeldung ebenfalls zu Beeinträchtigungen der Unabhängigkeit führen.

3.2 Europäische und internationale Entwicklungen

3.2.1 Safe Harbor

Sofern nicht bestimmte Ausnahmetatbestände des § 4c Abs. 1 BDSG vorliegen, sind Datenübermittlungen in das außereuropäische Ausland, welches über kein angemessenes Datenschutzniveau verfügt, nur zulässig, wenn ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gemäß § 4c Abs. 2 BDSG vorliegen. Diese Garantien könnten durch Verwendung sogenannter Standardvertragsklauseln, verbindlicher Unternehmensregelungen oder Einzelverträge geschaffen werden. Auch die Safe-Harbor-Entscheidung der Europäischen Kommission (Abl. L 215 vom 25. August 2000, S. 7) sollte für Unternehmen aus den USA die Möglichkeit bieten, entsprechende Garantien zu geben.

Bereits im XI. Tätigkeitsbericht (Nr. 3.1.1) wies der Landesbeauftragte auf die datenschutzrechtliche Problematik im Zusammenhang mit der Safe-Harbor-Entscheidung der Europäischen Kommission hin. Er kritisierte insbesondere, dass US-Unternehmen sich selbst gegenüber dem dortigen Handelsministerium verpflichteten, die Safe-Harbor-Prinzipien einzuhalten und sich damit selbst einen angemessenen Datenschutz gemäß der Europäischen Datenschutzrichtlinie attestieren konnten. Zudem vertrat der Landesbeauftragte die Ansicht, dass angesichts der bekannt gewordenen Informationen zu umfassenden und anlasslosen Überwachungsmaßnahmen von Geheimdiensten kein angemessenes Datenschutzniveau gewährleistet werde. Hierauf wies auch die Datenschutzkonferenz in ihrer Entschließung vom 18. und 19. März 2015 hin (**Anlage 22**).

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 6. Oktober 2015 (Rs. C-362/14, ZD 2015, 539) die Safe-Harbor-Entscheidung der Kommission aufgehoben. Kläger in diesem Verfahren war ein österreichischer Facebook-Nutzer. Wie bei allen Facebook-Nutzern (auch den zahlreichen aus Sachsen-Anhalt) wurden auch seine personenbezogenen Daten von der irischen Tochtergesellschaft an Server, die sich in den USA befinden, übermittelt und dort verarbeitet. Zuvor hatte die irische Datenschutzbehörde seine Beschwerde mit der Begründung zurückgewiesen, die Kommission habe in ihrer Safe-Harbor-Entscheidung festgestellt, dass die USA im Rahmen von Safe Harbor ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisten.

In seiner Entscheidung stellt der EuGH zunächst fest, dass die Existenz einer Entscheidung der Kommission, in der festgestellt wird, dass ein Drittland ein angemessenes Datenschutzniveau gewährleistet, die Befugnisse der Aufsichtsbehörden nicht beschränke. Daraus folgt, dass die Datenschutzbehörden ungeachtet von Kommissionsentscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen.

Weiterhin stellt der EuGH fest, dass eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, ohne irgendeine Einschränkung, Differenzierung oder Ausnahme festzulegen, den Wesensgehalt des durch Art. 7 der Grundrechtecharta garantierten Grundrechts auf Achtung des Privatlebens verletze. Zusätzlich sei der Wesensgehalt des in Art. 47 der Grundrechtecharta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt, da nach der Safe-Harbor-Entscheidung keine Möglichkeiten für den Bürger vorgesehen sind, mittels Rechtsbehelf Zugang zu den ihn betreffenden Daten zu erlangen bzw. ihre Berichtigung oder Löschung zu erwirken.

Durch dieses Urteil wird deutlich, dass Datenübermittlungen in die USA, die sich ausschließlich auf Safe Harbor stützen, nicht zulässig sind. Der Landesbeauftragte wird, sofern er Kenntnis von derartigen Übermittlungen erlangt, diese untersagen. Die Entscheidung dürfte sich auch auf die Verwendung von Standardvertragsklauseln, verbindlichen Unternehmensregelungen oder Einzelverträgen auswirken. Vieles spricht dafür, dass auch hier die Datenübermittlungen problematisch sein können. In diese Richtung zielt auch das Positionspapier der Datenschutzkonferenz vom 26. Oktober 2015[2].

Unternehmer sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer in Drittstaaten zu überprüfen und entsprechend den Anforderungen des EuGH-Urteils zu gestalten. Von Bedeutung könnte sein, ob in den unterschiedlichen Vertragswerken bestimmte technische und organisatorische Maßnahmen zugesichert werden, die einen unverhältnismäßigen Zugriff von Sicherheitsbehörden praktisch ausschließen. Bei Nutzung einer Cloud eines amerikanischen Anbieters wäre die Orientierungshilfe „Cloud Computing“ vom 9. Oktober 2014 der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises zu beachten. Bei sogenannten Storage-Diensten wird insbesondere die Inhaltsverschlüsselung empfohlen, bei der der Cloud-Anbieter keinen Zugriff auf den Schlüssel hat. Durch geeignete Wahl von Algorithmen und Schlüssellängen kann man hier einen langwährenden Schutz erreichen.

Die Europäische Kommission verhandelte mit den USA über ein neues Abkommen, welches die Safe-Harbor-Entscheidung ablösen soll. In ihrem oben erwähnten Positionspapier vom 26. Oktober 2015 hat die Datenschutzkonferenz die Kommission aufgefordert, auf die Schaffung weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit.

Die Verlautbarung der Europäischen Kommission von Anfang Februar 2016 lässt Zweifel bestehen, ob in dem beabsichtigten Nachfolgeabkommen „EU-US Privacy Shield“ die Vorgaben des Urteils des EuGH vom 6. Oktober 2015 umfassend berücksichtigt werden. Dies betrifft insbesondere die Durchsetzung der Betroffenenrechte vor US-Gerichten; ein Ombudsmann dürfte nicht ausreichend sein. Auch stellt sich die Frage nach der Verbindlichkeit des Abkommens und damit der Verhinderung massenhafter Zugriffe von US-Sicherheitsbehörden. Die Artikel 29-Gruppe begleitet

[2] http://lsaurl.de/SafeHarborUrteil

den Verhandlungsprozess kritisch; einstweilen werde die Anwendung von Standardvertragsklauseln und verbindlichen Unternehmensregelungen weiter geduldet.

3.2.2 FATCA

Im XI. Tätigkeitsbericht (Nr. 3.2.2) berichtete der Landesbeauftragte über FATCA. Dies ist ein Gesetz der USA, mit welchem Meldepflichten für Finanzinstitute in aller Welt eingeführt wurden, in Bezug auf Konten von in den USA steuerpflichtigen Personen und Gesellschaften.

Mit einem Bundesgesetz vom 18. Dezember 2013 wurde dafür die rechtliche Übermittlungsgrundlage in § 117c Abgabenordnung (AO) geschaffen (BGBl. I S. 4318, 4333). Dabei verweist § 117c AO auf § 150 Abs. 6 AO, wodurch sichergestellt ist, dass ein sicheres Verfahren für die Übermittlung der Daten angewandt wird, welches die Integrität und die Vertraulichkeit der Daten gewährleistet.

3.2.3 Flugpassagierdaten

Wie im XI. Tätigkeitsbericht (Nr. 3.2.3) bereits vermutet, wurden auch im vergangenen Berichtszeitraum weitere Abkommen zur Übermittlung von Flugpassagierdaten zwischen der Europäischen Union und verschiedenen Ländern geschlossen. So besteht nunmehr auch ein Abkommen mit Kanada und Mexiko. Aber auch Russland hat Interesse an einem solchen Abkommen gezeigt. Hier konnte die Übermittlung bisher auf die Daten beschränkt werden, die ohnehin aus einem Pass auslesbar sind.

Die Kritik der Datenschutzbeauftragten an diesen Abkommen besteht noch immer in der anlasslosen langen Speicherung von vielen verschiedenen Datensätzen und deren Auswertungsmöglichkeiten.

Durch die aktuellen Entwicklungen in der Welt, vor allem die Attentate und Terroranschläge in Paris, gaben nunmehr weitere EU-Abgeordnete ihren Widerstand gegen die Flugpassagierdatenübermittlung auf. Dabei wird auch wieder über ein innereuropäisches System des Datenaustausches zur Terrorabwehr gesprochen. Eine Speicherung der Daten sollte in einem solchen System nur 30 Tage unter dem Klarnamen des Reisenden gestattet werden. Jedoch wurde diese kurze Speicherfrist unter dem Eindruck der Terroranschläge in Paris gekippt.

Die EU-Innenminister haben nunmehr den Weg für eine Flugpassagierdatenspeicherung freigemacht, wonach jeder Staat eine Kontaktstelle aufbaut, welche die Daten aller Fluggesellschaften seines Landes speichert und mit den anderen Ländern austauscht. Dies soll erst einmal für außereuropäische Flüge verbindlich sein und für innereuropäische Flüge auf freiwilliger Basis erfolgen.

Der Abschluss einer dementsprechenden Vereinbarung bleibt abzuwarten.

3.2.4 System der Bankdatenauswertung – SWIFT

In seinem XI. Tätigkeitsbericht (Nr. 3.2.1) berichtete der Landesbeauftragte von Bestrebungen des Europäischen Parlaments, das bestehende Abkommen zu SWIFT

mit den Vereinigten Staaten auszusetzen, da wohl auch die NSA auf die Daten des SWIFT-Netzwerkes zugriffen, ohne dass es den Nutzern bekannt wurde.

SWIFT leitet weltweit Transaktionen zwischen Banken, Börsen und anderen Finanzinstituten weiter. Über dieses System werden nicht nur der Zahlungsverkehr abgewickelt, sondern auch Nachrichten zwischen den Firmen und den Finanzinstituten übermittelt.

Eine Prüfung der Datenschutzanforderungen durch den Europol Joint Supervisory Body im Rahmen von Abfragen von Terrorfahndern der Vereinigten Staaten hatte in der Vergangenheit ergeben, dass eine Überprüfung einzelner Vorgänge unmöglich ist, da Begründungen teilweise nur mündlich erfolgten.

Das Abkommen selbst wurde jedoch nicht aufgekündigt, da die Übermittlung der Daten als wichtiger Bestandteil zur Aufdeckung der Zahlungsströme der Terrorismusfinanzierung gesehen wird.

3.2.5 Transatlantische Freihandelsabkommen

Im Jahr 2013 verkündeten der Präsident der EU-Kommission José Manuel Barroso und der US-Präsident Barack Obama am Rande des G8-Gipfeltreffens in Nordirland, eine Freihandelszone schaffen zu wollen, in der die Wirtschaft durch den Abbau von Zöllen und Handelshemmnissen gestärkt und durch die Schaffung von gemeinsamen Standards die Vorherrschaft im Welthandel gesichert wird.

Seit Verkündung dieses Vorhabens schreiten die Verhandlungen zur Transatlantic Trade and Investment Partnership (TTIP) stetig voran. Nach Medienberichten sollen sich die USA im Rahmen der Verhandlungen für eine Absenkung der derzeitigen Datenschutzstandards eingesetzt haben. Ob und inwieweit der Datenschutz nach dem Safe Harbor-Urteil des EuGH noch Gegenstand der Verhandlungen ist, ist unklar. Genaue Angaben über den Verhandlungsstand sind nicht bekannt, da die Verhandlungen bisher weitestgehend im geheimen stattfanden und erst langsam an einer Verbesserung der Transparenz gearbeitet wird (vgl. Nr. 2.3 des III. Tätigkeitsberichts zur Informationsfreiheit).

Gleiches gilt für das ebenfalls geplante Dienstleistungsabkommen Trade in Service Agreement (TISA). Hinsichtlich TISA soll der Handelsausschuss des EU-Parlaments mittlerweile für weitreichende Korrekturen gestimmt haben. Er soll nun verlangen, dass Daten von europäischen Bürgern nur dann grenzüberschreitend weitergegeben werden dürfen, wenn EU-Datenschutz und Sicherheitsbestimmungen gewahrt sind.

3.2.6 Schengener Informationssystem II

Bereits in seinem XI. Tätigkeitsbericht (Nr. 3.2.4) beschrieb der Landesbeauftragte das sich lange hinziehende Verfahren zur Einführung des Schengener Informationssystems II (SIS II), also der zweiten Generation.

Nunmehr ist diese Erweiterung des ursprünglichen Systems in der Praxis erprobt. Es sind 28 Systeme der Schengen-Mitgliedstaaten angeschlossen. Die Einzeldaten stehen den anderen Mitgliedstaaten bereits Sekunden nach der Eingabe zur Verfügung.

Im SIS II können nunmehr auch weitaus mehr Daten eingegeben werden, so auch biometrische Daten wie Fingerabdrücke und Passbilder.

Des Weiteren können verschiedene Optionen miteinander verknüpft werden. Konnte bisher nur nach bestimmten Personen oder vermissten Gegenständen wie z. B. Fahrzeugen, Kreditkarten oder Pässen und anderen Dokumenten gefahndet werden, können nunmehr zahlreiche Verknüpfungsmöglichkeiten genutzt werden. Dadurch ist das SIS II zu einem echten Recherchesystem geworden.

Für die Kontrolle der Ausschreibungen im System auf europäischer Ebene ist mit Einführung von SIS II der Europäische Datenschutzbeauftragte zuständig, der gemäß Beschluss über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) mit den nationalen Kontrollinstanzen im Rahmen der jeweiligen Zuständigkeit aktiv zusammenarbeiten muss. Dieses Kontrollgremium trifft mindestens zweimal jährlich zusammen. Die Vertretung der deutschen Kontrollgruppe in diesem Gremium wird durch einen Vertreter der BfDI und einen Vertreter der Landesbeauftragten (Mitarbeiterin des hessischen LfD) wahrgenommen.

3.2.7 Umbrella Agreement

In seinem X. Tätigkeitsbericht (Nr. 7.3) berichtete der Landesbeauftragte über die Bestrebungen, ein Datenschutzabkommen zwischen der EU und den Vereinigten Staaten zu Stande zu bringen. Dieses Rahmenabkommen soll die datenschutzrechtliche Grundlage für Datenübermittlungen an die Vereinigten Staaten zu Strafverfolgungszwecken bilden. Dabei sollen nicht nur zukünftige Vereinbarungen Berücksichtigung finden, sondern auch bereits bestehende Abkommen.

Bisher bestehen zu verschiedenen Bereichen Einzelabkommen, wie z. B. zu SWIFT (vgl. Nr. 3.2.4), zur Übermittlung von Flugpassagierdaten (vgl. Nr. 3.2.3) sowie der Datenaustausch mit Europol und Eurojust und weitere Abkommen zur Kooperation zwischen Strafverfolgungsbehörden.

Im September 2015 wurde nunmehr bekannt, dass dieses Datenschutz-Rahmenabkommen, welches als „Umbrella Agreement“ bezeichnet wird, vor dem Abschluss steht. Jedoch muss dieses Abkommen weitere Hürden nehmen, bis es in Kraft tritt. So müssen unter anderem auch in den Vereinigten Staaten die rechtlichen Bedingungen geschaffen werden, unter welchen auch EU-Bürger das Recht haben, Klage aufgrund von Datenschutzverstößen bei US-Gerichten einreichen können.

Kritisch zu betrachten ist, wie auch die BfDI in ihrem 25. Tätigkeitsbericht betont, dass durch das Umbrella Agreement nur die Datenübermittlungen zwischen den Strafverfolgungsbehörden abgedeckt werden. Das heißt, dass die Daten, die von den US-Sicherheitsbehörden verarbeitet werden, nicht unter den Schutz des Umbrella Agreements fallen.

3.2.8 Internationale Datenschutzkonferenzen

Die 36. Internationale Konferenz der Datenschutzbehörden fand vom 13. bis 16. Oktober 2014 in Balaclavia, Mauritius statt.

Neben einer Grundsatzentschließung zum Dialog der Datenschützer bei der Verstärkung des Datenschutzes im Digitalen Zeitalter (**Anlage 42**) betraf ein anderes wichtiges Thema auf dieser Konferenz das „Internet der Dinge“. In einer Entschließung (**Anlage 43**) äußerten die Datenschutzbehörden ihre Besorgnis, das durch die Verwendung immer kleinerer Sensoren in immer kleineren Geräten immer mehr Daten in hoher Qualität und Quantität von einzelnen Personen gesammelt werden, welche auch die finanziellen Interessen vieler Unternehmen wecken. Das Interesse liegt vor allem in den neuen Diensten, welche im Zusammenhang mit dem Internet der Dinge angeboten werden können. Die Datenschutzbehörden wollen auf die Sicherheitsrisiken aufmerksam machen. So sollte eine Datenverarbeitung auf das jeweilige Endgerät selbst beschränkt werden oder eine Ende-zu-Ende-Verschlüsselung bei der Übertragung der Daten genutzt werden.

In einer weiteren Entschließung gehen die Datenschutzbehörden auf die Verwendung personenbezogener Daten bei Big Data (**Anlage 44**) ein. Dabei betonen die Datenschutzbehörden, dass der Schutz der personenbezogenen Daten durch Datenschutzgrundsätze wie z. B. der Grundsatz der Zweckbindung und der Datenvermeidung wichtiger ist als je zuvor, da immer mehr Informationen zu jeder einzelnen Person gesammelt werden.

Die 37. Internationale Konferenz der Datenschutzbehörden, die vom 26. bis 29. Oktober 2015 in Amsterdam zusammen kam, diskutierte die Möglichkeit der Brückenbildung insbesondere zwischen Europa und den USA mittels Datenschutzstandards und Optionen für eine stärkere Kooperation der Datenschützer. Eine Resolution unterstützt die Zusammenarbeit mit dem Sonderberichterstatter für den Datenschutz der Vereinten Nationen (**Anlage 45**).

3.2.9 Europäische Datenschutzkonferenzen

Am 5. Juni 2014 tagten die europäischen Datenschutzbehörden auf Einladung der französischen Datenschutzbehörde (CNIL) und des Europarates in Straßburg.

Dabei befassten sie sich vorrangig mit der Modernisierung der Europaratskonvention 108, des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten aus dem Jahr 1981.

Die Datenschutzbehörden fassten eine Entschließung (**Anlage 40**), um ihre Forderung zu unterstreichen, *„dass jede Absenkung des derzeit durch das Übereinkommen 108 und seines Protokolls gewährleisteten Schutzes einen Rückschritt darstellen würde“*. Gleichzeitig hebt die Konferenz der europäischen Datenschutzbeauftragten hervor, *„dass ein effektiver Datenschutz die Schaffung unabhängiger Aufsichtsbehörden erfordert“.*

Die Konferenz der europäischen Datenschutzbehörden forderte bei ihrer Tagung in Manchester vom 18. bis 20. Mai 2015 die Regierungen der europäischen Länder auf, für die Erfüllung datenschutzrechtlicher Erwartungen in der digitalen Zukunft dafür Sorge zu tragen, dass die finanzielle Ausstattung der Datenschutzbehörden den wachsenden Anforderungen gerecht wird, wobei die notwendige Unabhängigkeit respektiert und aufrechterhalten werden muss (**Anlage 41**).

3.2.10 Europäischer Datenschutztag

Der Europarat hat den 28. Januar als jährlich zu begehenden Datenschutztag ausgerufen, um das Bewusstsein für den Datenschutz in Europa zu stärken (siehe IX. Tätigkeitsbericht, Nr. 3.3). Demgemäß begingen die Datenschutzbeauftragten des Bundes und der Länder auch im Januar 2014, 2015 und 2016 diesen Tag mit einer zentralen Veranstaltung. Mit Vorträgen und Diskussionen von Fachleuten aus Politik, Verwaltung und Wissenschaft konnte öffentlichkeitswirksam über aktuelle Themen informiert werden. Inhaltliche Schwerpunkte betrafen die Nachrichtendienste in Zeiten von Big Data und den Umgang mit unterschiedlichen Datenschutzniveaus zwischen der Europäischen Union und den Vereinigten Staaten von Amerika im Lichte der Europäischen Datenschutz-Grundverordnung.

4 Technik und Organisation

4.1 IT-Planungsrat

In seinem XI. Tätigkeitsbericht (Nr. 4.1) hatte der Landesbeauftragte über die datenschutzrelevanten Themen des Aktionsplans 2013 des *IT-Planungsrates* (IT-PLR) sowie über die Bildung des *IKT-Rates* auf Landesebene berichtet. Der Landesbeauftragte ist seit 2012 beratendes Mitglied im IKT-Rat. Im Rahmen der Sitzungen des IKT-Rates erfolgte schwerpunktmäßig die Vorbereitung der Voten des Landes für die Beschlüsse des IT-PLR. Leider ist festzustellen, dass aufgrund des oft engen Zeitrahmens zur Vorbereitung der Sitzungen des IT-PLR eine inhaltliche Befassung auch mit datenschutzrechtlichen Themen nicht in dem erforderlichen Maße im IKT-Rat stattgefunden hat. Mehrere Sitzungen des IKT-Rates fielen kurzfristig aus. Als Folge konnten die Voten des Landes nur unter entsprechendem Zeitdruck und nur im Umlaufverfahren gefasst werden. Eine strategische Debatte zur zukünftigen IT-Landschaft Sachsen-Anhalts fand schon gar nicht statt.

Der Aktionsplan des IT-PLR wurde jährlich fortgeschrieben. Der aktuelle Aktionsplan 2015 wurde auf der 15. Sitzung des IT-PLR am 16. Oktober 2014 beschlossen. Im Berichtszeitraum nahm der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern als Vertreter der Länder, neben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, an den Sitzungen des IT-PLR beratend teil. Dieser hat mittlerweile zahlreiche Arbeits-, Projekt- und Kooperationsgruppen eingesetzt, die Steuerungs- und Koordinierungsprojekte federführend begleiten und Anwendungen des IT-PLR umsetzen sollen. Vertreter der Datenschutzbehörden sind u. a. im Beirat der Koordinierungsstelle für IT-Standards, in der Kooperationsgruppe Informationssicherheit, in der Projektgruppe eID-Strategie und in der Arbeitsgruppe Netzsicherheit tätig. Die zeitlichen und personellen Ressourcen des Landesbeauftragten lassen allerdings derzeit eine Mitarbeit in diesen Arbeitsgremien des IT-PLR nicht zu.

Beratungsschwerpunkte des IT-PLR mit besonderem Datenschutzbezug bildeten die Umsetzungen der E-Government-Vorhaben, welche sich an der *Nationalen E-Government-Strategie* (NEGS) orientieren, die für den Zeitraum bis 2015 beschlossen wurde. Hierzu zählen nachfolgende wesentliche ***Steuerungsprojekte*** des IT-PLR, deren Zuweisung durch den Chef des Bundeskanzleramts und die Chefinnen und Chefs der Staats- und Senatskanzleien der Länder auf der Grundlage von

§ 1 Abs. 1 Satz 1 Nr. 3 des Vertrags über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Art. 91c GG (IT-Staatsvertrag) erfolgte:

- Umsetzung der Leitlinie für *Informationssicherheit* (Federführung: Bayern; Abschluss: 31. Dezember 2017),

- Umsetzung der *eID-Strategie* für E-Government (Federführung: Bund; Abschluss: 31. Dezember 2017),

- *Föderales Informationsmanagement* (FIM) (Federführung: Bund, Sachsen-Anhalt; Abschluss: 31. Dezember 2015).

Der IT-PLR hat sich im zurückliegenden Berichtszeitraum mehrfach mit dem Thema der Umsetzung der **Leitlinie für Informationssicherheit** befasst. Auf seiner 12. Sitzung am 2. Oktober 2013 hat er mit der Verabschiedung des Aktionsplanes 2014 ein neues Steuerungsprojekt „Umsetzung der Leitlinie für Informationssicherheit“ beschlossen. Diese Leitlinie hat für den kommunalen Bereich nur empfehlenden Charakter. Auch ein nochmaliger Vorstoß der kommunalen Spitzenverbände im Juli 2014, diese Leitlinie auch für den kommunalen Bereich für verbindlich zu erklären, hatte keinen Erfolg und kam als Beschluss des IT-PLR nicht zustande. Unter den elf „Nein-Stimmen“ befand sich auch Sachsen-Anhalt. Dieser Umstand ist auch aus datenschutzrechlicher Sicht unbefriedigend, denn gerade im kommunalen Bereich darf keine Absenkung des Informationssicherheitsniveaus zugelassen werden. „Klassenunterschiede“ hinsichtlich der Informationssicherheit darf es zwischen dem Land und den Kommunen nicht geben.

Bei der Verabschiedung der **eID-Strategie** und der dazu erhobenen Kritik der Landesdatenschutzbeauftragten im Hinblick auf eine unzureichende Berücksichtigung der Datenschutzaspekte forderte der IT-PLR in seiner 12. Sitzung am 2. Oktober 2013 in einem Beschluss zur Umsetzung der Maßnahmen der eID-Strategie zur Berücksichtigung der Erfordernisse des Datenschutzes auf. Zur Umsetzung der eID-Strategie für E-Government besteht u. a das Ziel im Bund, in den Ländern und Kommunen auf Ebene der Behörden bis spätestens Ende 2016 den elektronischen Zugang zu Verwaltungsdienstleistungen mit der eID-Funktion des neuen Personalausweises und mit De-Mail zu eröffnen. Eine entsprechende Strategie für Sachsen-Anhalt ist dem Landesbeauftragten hierzu bisher nicht bekannt.

Mit dem **Projekt FIM** soll eine nachhaltige Infrastruktur auf fachlicher und organisatorischer Ebene geschaffen werden, welche Informationen zu Verwaltungsverfahren umfasst. In Kooperation mit den Vorhaben *LeiKa* (Leistungskatalog der öffentlichen Verwaltung) und *Nationale Prozessbibliothek* (Verzeichnis aller deutschen Verwaltungsprozesse) soll damit eine für alle Ebenen der öffentlichen Verwaltung gemeinsame Infrastruktur entstehen. Mit der Umsetzung des FIM-Standardisierungskonzepts wird eine wichtige Voraussetzung für die effiziente und effektive Erstellung sowie den Betrieb von E-Government-Anwendungen aller föderalen Ebenen geschaffen. Ab 2016 soll dieses Steuerungsprojekt in die Betriebsphase überführt werden.

In Wahrnehmung der Aufgaben als Koordinierungsgremium hatte der IT-PLR auf seiner 16. Sitzung am 18. März 2015 gemäß § 4 Abs. 1 Nr. 4 des Gesetzes über die

Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Art. 91c Abs. 4 GG – vom 10. August 2009 (ITNetzG) die *Anschlussbedingungen* für das Verbindungsnetz beschlossen. Allerdings wird die Umsetzung dieser Anschlussbedingungen erst bis zum 31. Dezember 2017 erfolgen. Nach § 3 ITNetzG sollte aber der Datenaustausch zwischen Bund und Ländern über das Verbindungsnetz bereits ab dem 1. Januar 2015 realisiert werden. Gegenwärtig wird das Verbindungsnetz vom Deutschland Online Infrastruktur e. V. (DOI) betrieben. Die Neubeauftragung des Verbindungsnetzes („DOI 2.0“) erfolgt im Rahmen des Programms „Netze des Bundes“. Der gültige Rahmenvertrag mit dem Provider T-Systems International konnte nochmals bis 31. März 2015 mit der Maßgabe verlängert werden, die vereinbarten Leistungen über einen Zeitraum von einem Jahr weiter zur Verfügung zu stellen, bis zu einer Migration auf eine Nachfolgeplattform. Angesichts der Beschlussfassung des ITNetzG bereits im Jahr 2009 war die nunmehr eingetretene Verzögerung der Inbetriebnahme des Verbindungsnetzes auch aus datenschutzrechlicher Sicht kritisch zu bewerten, geht es bei diesem wichtigen Projekt des Bundes doch um das Vertrauen von Bürgerinnen und Bürgern sowie der Wirtschaft in sichere Übertragungswege.

Weiterhin betreut der IT-PLR eine Reihe von **Koordinierungsprojekten**. Dabei nimmt der IT-PLR für diese Vorhaben die Koordinierungsverantwortung für die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik nach § 1 Abs. 1 Satz 1 Nr. 1 des IT-Staatsvertrages wahr. Zu den Koordinierungsvorhaben mit Datenschutzbezug gehören u. a.:

- Nationales Waffenregister – Stufen 2 und 3 (Federführung: Bund, Baden-Württemberg; Auftraggeber: Innenministerkonferenz; Abschluss: 31. Dezember 2017),

- SAFE (Secure Access to Federated e-Justice/e-Government) (Federführung: Baden-Württemberg; fachlich verantwortlich: Justizministerkonferenz; Abschluss: 31. Dezember 2015),

- EDV-Grundbuch (Entwicklung eines bundeseinheitlichen Datenbankgrundbuchs) (Federführung: Bayern, Auftraggeber: Justizministerkonferenz; Abschluss: 31. Dezember 2016),

- Einheitlicher Ansprechpartner – EA2.0 (Federführung: Bund, Hessen; Analyse und Überprüfung der strategischen Ausrichtung des EA-Systems sowie Anpassung an neue Rahmenbedingungen; Abschluss: 31. Dezember 2015).

Darüber hinaus unterstützt der IT-PLR neben dem Betrieb von **Anwendungen** (wie z. B. dem Deutschen Verwaltungsdiensteverzeichnis (Federführung: Bund), Behördenfinder Deutschland (Federführung: Sachsen-Anhalt), Leistungskatalog (Federführung: Sachsen-Anhalt), Governikus – sicherer und nachvollziehbarer Datenaustausch von Verwaltungen, Unternehmen und Einzelpersonen über das Internet (Federführung: Bremen)) die Maßnahmen zur Verbesserung der Rahmenbedingungen des E-Governments.

Zur **Verbesserung von Rahmenbedingungen des E-Governments** gehören die Analyse und Verbesserung der rechtlichen und organisatorischen Bedingungen u. a zur Umsetzung des E-Government-Gesetzes des Bundes und der Transfer in die

Länder sowie die Begleitung des Normenscreenings. Ein weiteres Schwerpunktthema bildet die Maßnahme **Föderale IT-Kooperation (FITKO)**, deren Ziel es ist, die föderale Zusammenarbeit in der Informationstechnik zu fördern und zu verbessern. Die umfassende Zusammenarbeit in der Informationstechnik zwischen Bund und Ländern, die durch Art. 91c GG ermöglicht wird, ist bisher operativ nicht umgesetzt. Sie bedarf nach Einschätzung der durch den IT-PLR dazu eingesetzten Bund-Länder-Arbeitsgruppe FITKO einer Professionalisierung, verbunden mit der Bildung einer eigenen Organisationsstruktur durch die Einrichtung einer gemeinsamen Bund-Länder-Organisation. Diese soll als Abteilung oder Stabsstelle bei einer Landes- oder Bundesbehörde eingerichtet werden. Der IT-PLR hat dazu in einem Beschluss seiner 17. Sitzung im Juni 2015 die Bund-Länder-Arbeitsgruppe FITKO mit der Vorlage eines Entwurfs für ein Verwaltungsabkommen zur 19. Sitzung im März 2016 beauftragt.

Auch in Bezug auf das Steuerungsprojekt „Umsetzung der eID-Strategie für E-Government“ hat sich der IT-PLR in seiner 17. Sitzung für eine flächendeckende Verbreitung von **Bürgerkonten** und deren datenschutzgerechten Einsatz ausgesprochen und die Projektgruppe eID-Strategie bis zu seiner 19. Sitzung um die Definition notwendiger rechtlicher Rahmenbedingungen als Voraussetzung von Interoperabilität der Bürgerkonten gebeten. Nach dem Statusbericht der Projektgruppe eID-Strategie vom April 2015 werden bereits in elf Ländern solche temporären und permanenten Bürgerkonten angeboten, in drei Ländern sollen diese in Planung sein. Für Sachsen-Anhalt sind dem Landesbeauftragten hierzu bisher keine Aktivitäten bekannt. In diesem Zusammenhang erinnert der Landesbeauftragte die Landesregierung, gemäß § 14 Abs. 1 Satz 2 DSG LSA *rechtzeitig* über grundlegende Planungen zum Aufbau oder zur Änderung automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten.

Auf seiner 18. Sitzung am 1. Oktober 2015 hat der IT-PLR die Fortschreibung der NEGS sowie bis auf Weiteres die Fortführung der Koordinierungsgruppe „Strategie“ beschlossen. Zu den Aufgaben dieser Koordinierungsgruppe gehören u. a. die Evaluation der NEGS nach jeweils drei, spätestens nach jeweils fünf Jahren sowie deren regelmäßige Aktualisierung.

Im Zielbereich C „Informationssicherheit und Datenschutz“ zählen hierzu Schutzmaßnahmen zur Gewährleistung der Informationssicherheit bei allen Kommunikationspartnern, d. h. sowohl bei Bürgerinnen und Bürgern als auch bei Wirtschaft und Verwaltung. Darüber hinaus ist der technische und organisatorische Datenschutz zu gewährleisten, indem eine Ausrichtung an den Schutzzielen Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Nichtverkettbarkeit (zur technischen Sicherung der Zweckbindung) und Intervenierbarkeit (als technische Gestaltung zur Ausübung von Betroffenenrechten) erfolgen soll. Diese Ausrichtung an den modernen Regelungszielen erfordert eine Anpassung der rechtlichen, technischen und organisatorischen Rahmenbedingungen. Der Landesbeauftragte geht davon aus, dass diese Grundsätze der fortgeschriebenen NEGS Berücksichtigung bei der Ausarbeitung eines E-Government-Gesetzes des Landes finden werden (vgl. Nr. 4.3).

Der IT-PLR hat schließlich in einer Sondersitzung am 30. November 2015 die „Digitalisierung des Asylverfahrens zwischen Bund und Ländern“ als neues Koordinierungsprojekt in seine Agenda aufgenommen. Der Entwurf der Bundesregierung für ein Datenaustauschverbesserungsgesetz regelt einen umfassenden zentralen Da-

tenbestand im Ausländerzentralregister sowie einen Ankunftsnachweis für Asyl- und Schutzsuchende (BT-Drs. 18/7203, BR-Drs. 25/16); das Gesetz vom 2. Februar 2016 wurde am 4. Februar 2016 verkündet (BGBl. I S. 130).

4.2 Landesleitlinie Informationssicherheit verzögert sich

In seinem XI. Tätigkeitsbericht (Nr. 4.3) hatte der Landesbeauftragte über den Stand der Erarbeitung einer Landesleitlinie Informationssicherheit im Zusammenhang mit der Verabschiedung der IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“ vom 10. Oktober 2012 (MBl. LSA S. 585) berichtet. Zu der angekündigten Fortsetzung der Ausarbeitung noch im 2. Halbjahr 2013 durch das federführende Ministerium der Finanzen des Landes Sachsen-Anhalt ist es aber bisher nicht gekommen. Zum einen verabschiedete der IT-Planungsrat (IT-PLR) selbst bereits im März 2013 seine Leitlinie Informationssicherheit einschließlich des Umsetzungsplanes, die für alle Behörden des Bundes und der Länder Geltung besitzt und deren Vorgaben auch in der Landesleitlinie Berücksichtigung finden müssen. Zum anderen ließ die seit 2014 angespannte Personalsituation in der Abteilung 6 des Ministeriums der Finanzen des Landes Sachsen-Anhalt, verursacht durch deren neue Aufgaben mit dem rückwirkenden Beitritt des Landes zum 1. Januar 2013 zur rechtsfähigen Anstalt des öffentlichen Rechts Dataport und der damit verbundenen Funktion als ein Trägerland dieser Anstalt, eine zügige Weiterarbeit an der Landesleitlinie Informationssicherheit nicht zu. Insbesondere die Überleitung der automatisierten Verfahren der Finanzverwaltung zum Data Center Steuern in Rostock und auch der ehemals im Landesrechenzentrum betriebenen Fachverfahren der Ressorts zu Dataport beanspruchten die personellen Kapazitäten der Abteilung 6 des Ministeriums der Finanzen des Landes Sachsen-Anhalt. Die Planung und der Aufbau eines modernen Sprach- und Datennetzes (ITN-XT) für die Landesverwaltung, als das zentrale Projekt der IKT-Strategie, banden ebenfalls personelle Ressourcen.

Auch wenn die Anschlussbedingungen für das Verbindungsnetz, die eine verbindliche Wirkung für Bund und Länder haben, nach einem Beschluss der 16. Sitzung des IT-PLR im März 2015 erst spätestens bis zum 31. Dezember 2017 umzusetzen sind, sollte die Weiterarbeit an der Landesleitlinie Informationssicherheit nicht auf den „Sankt-Nimmerleins-Tag“ verschoben werden. Spätestens mit der Ausarbeitung eines E-Government-Gesetzes für das Land bedarf es hier grundlegender und verbindlicher Festlegungen auch unter Berücksichtigung des Datenschutzes. Eine gute Grundlage bietet weiterhin der seit Februar 2011 vorliegende Entwurf der Landesleitlinie, an dem der Landesbeauftragte mitgewirkt hatte.

4.3 E-Government-Gesetzgebung in Sachsen-Anhalt

Der Landesbeauftragte hatte in seinem XI. Tätigkeitsbericht (Nr. 4.3) über die im Oktober 2012 von der Landesregierung beschlossene IKT-Strategie „Sachsen-Anhalt digital 2020“, an deren Ausarbeitung er aktiv beteiligt war, berichtet. Für deren zukünftige Umsetzung empfahl der Landesbeauftragte bereits damals, ein E-Government-Gesetz des Landes zu schaffen. Durch das am 1. August 2013 in Kraft getretene Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG) des Bundes vom 25. Juli 2013 (BGBl. I S. 2749) bestand danach auch in Sachsen-Anhalt Handlungsbedarf. Bereits seit dem Vorjahr befasste sich eine mit Beschluss des Landtages vom 22. März 2012 (LT-Drs. 6/968)

eingesetzte Enquete-Kommission zum Thema „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“ mit der Zukunft der öffentlichen Verwaltung und behandelte u. a. Themen wie Funktionalreform, Personalstruktur und E-Government sowie Open Government (Schwerpunkt 3 „E-Government-Strategie“ des Einsetzungsbeschlusses). Die Arbeit der Enquete-Kommission war auf einen Zeitraum von drei Jahren begrenzt.

Die Landesregierung hatte sich bereits bei der 12. Sitzung des IT-Planungsrates (IT-PLR) im Oktober 2013 in ihrem Votum zur „Umsetzung der eID-Strategie für E-Government“, einem Steuerungsprojekt des IT-PLR im Rahmen der Umsetzung der Nationalen E-Government-Strategie (NEGS), für eine entsprechende Umsetzung in Rechtsvorschriften des Landes ausgesprochen. In diesen sollten die Schriftform und explizit die qualifizierte elektronische Signatur (QES) angeordnet werden, analog den Regelungen des EGovG des Bundes. Bis Ende 2016 sollte dazu ein E-Government-Gesetz des Landes geschaffen werden, um neben der QES auch den neuen Personalausweis (nPA) mit seiner eID-Funktion und De-Mail zur Anwendung zu bringen. Des Weiteren, so die Landesregierung in ihrem damaligen Votum, erfordere die Umsetzung der eID-Strategie für E-Government, ebenfalls bis Ende 2016 für Behörden der Landes- und Kommunalverwaltung gleichermaßen den elektronischen Zugang zu Verwaltungsdienstleistungen mit der eID-Funktion des nPA und mit De-Mail zu eröffnen.

Folgerichtig wurde im Mai 2014 bei der 1. Aktualisierung des Umsetzungsplanes zur IKT-Strategie „Sachsen-Anhalt digital 2020“ als ein wesentliches Umsetzungsprojekt (Nr. 1) die Erarbeitung eines E-Government-Gesetzes für das Land Sachsen-Anhalt aufgenommen. Mit diesem sollten zum einen Regelungslücken des EGovG des Bundes geschlossen werden. Gleichzeitig sollten die Regelungen zur elektronischen Unterstützung der Verwaltung, wie im EGovG des Bundes bereits normiert, für eine eventuelle Übernahme und Anwendung für das Land überprüft werden. Das Sprichwort „Papier ist geduldig“ bewahrheitete sich leider für dieses Projekt des Umsetzungsplanes, denn seitens der Landesregierung waren in dieser Hinsicht keine weiteren grundlegenden Aktivitäten zu verzeichnen. Auch ein vom Ministerium für Inneres und Sport des Landes Sachsen-Anhalt initiierter Workshop "Folgerungen für Sachsen-Anhalt aus dem E-Government-Gesetz des Bundes“ im September 2014 brachte keinen wesentlichen Fortschritt für dieses Projekt.

Die fachliche Unterstützung und Begleitung der Enquete-Kommission des Landtages in Form von Stellungnahmen bildete für den Landesbeauftragten als Sachverständigen im Rahmen der durchgeführten Anhörungen der Enquete-Kommission und für seine Mitarbeiter während des gesamten Berichtszeitraums einen Schwerpunkt der Beratungstätigkeit. Im Rahmen der Anhörung am 7. November 2014 übergab der Landesbeauftragte seine *Kernempfehlungen* zum Schwerpunkt 3 „E-Government-Strategie“ des Einsetzungsbeschlusses der Enquete-Kommission (Vorlage 17, Ausschuss-Drs. 6/E07/7 vom 7. November 2014) (**Anlage 46**). Darin wird auch auf die Digitale Agenda 2014-2017 und das „Programm Digitale Verwaltung 2020“ der Bundesregierung Bezug genommen.

Nach dreijähriger Tätigkeit legte die Enquete-Kommission des Landtages von Sachsen-Anhalt am 1. September 2015 ihren Abschlussbericht vor (LT-Drs. 6/4331 vom 31. August 2015). Fraktionsübergreifend folgte sie dabei den Kernempfehlungen des Landesbeauftragten im Bereich des E-Governments, welche ergänzend auch Forde-

rungen zum Open-Government beinhalteten. Durch die Enquete-Kommission wurde mit diesem Abschlussbericht der Weg für eine offene, bürgernahe, digitale Verwaltung aufgezeigt.

Bestärkt in seinen Forderungen wurde der Landesbeauftragte durch das am 28. Oktober 2015 in Kraft getretene Gesetz über die Organisation der Landesverwaltung Sachsen-Anhalt (Organisationsgesetz Sachsen-Anhalt – OrgG LSA) vom 27. Oktober 2015 (GVBl. LSA S. 554). Der § 3 „Elektronische Verwaltung“ des Gesetzes trifft dazu entsprechende Regelungen. Da § 3 Abs. 3 des Gesetzes allerdings keinen Zeithorizont für die gesetzliche Regelung vorsieht, besteht Anlass zur Sorge, dass die Einführung eines E-Government-Gesetzes nicht mehr mit dem nötigen Nachdruck verfolgt werden wird. Allerdings ist zu beachten, dass das OrgG LSA, so hilfreich es auch sein mag, seiner Natur nach nur ein Programmgesetz bleibt. Seine konkrete Umsetzung durch ein E-Government-Gesetz für Sachsen-Anhalt unter Berücksichtigung von Regelungen zum Open-Government wäre noch viel wichtiger.

Zur Umsetzung der Vorschläge des Landesbeauftragten, welche sich die Enquete-Kommission des Landtages zu eigen gemacht hat, benötigt die Landesregierung eine ganzheitliche, nachhaltige, verbindliche, vernetzte und den Datenschutz und die Datensicherheit einbeziehende Strategie. Zukünftig sollte nicht mehr nur eine Technik-, sondern auch eine E-Government-Folgenabschätzung vorgenommen werden. Es sollte geprüft werden, welche Auswirkungen ein Vorhaben auf die E-Government-Strategie des Landes haben kann und wie Datenschutz und Datensicherheit dabei beachtet und umgesetzt werden müssen. Da die Vorschläge der Enquete-Kommission von allen Fraktionen mitgetragen wurden, sollte die Landesregierung nunmehr zügig mit der Umsetzung der Vorschläge beginnen. Die Empfehlungen könnten auch in eine Digitale Agenda des Landes Sachsen-Anhalt aufgenommen werden.

Sachsen-Anhalt steht damit bei der Umsetzung seiner E-Government-Strategie noch immer erst am Anfang, während der Bund mit seinem E-Government-Gesetz, dem Regierungsprogramm „Digitale Verwaltung 2020“ ebenso wie einige Länder, z. B. Sachsen, mit einem eigenen Landes-E-Government-Gesetz hier bereits wesentlich weiter sind. Nach Information des zuständigen Ministeriums für Inneres und Sport hat zum Ende der 6. Legislaturperiode zumindest auch die Erarbeitung eines Referentenentwurfs für das Land Sachsen-Anhalt begonnen. Der Landesbeauftragte soll rechtzeitig zu den inhaltlichen Schwerpunkten informiert und damit bei der Ausarbeitung des Entwurfes beteiligt werden.

Die verschlüsselte elektronische Kommunikation in und mit der Landesverwaltung (siehe Nr. 4.5) muss nach den Skandalen um die NSA in einem Landes-E-Government-Gesetz endlich gesetzlich geregelt werden. Die Schaffung, Umsetzung und Finanzierung von einheitlichen IKT-Standards im Bereich der Informationssicherheit und des Datenaustausches sind notwendig. Auch hier ist die kommunale Ebene in vollem Umfang einzubeziehen. Es muss zu einem Wandel in der Verwaltungskultur kommen. Die Landes- und Kommunalverwaltungen brauchen mehr E-Government-Kompetenz.

4.4 IT-Sicherheitsgesetz

Mit der weiter zunehmenden Digitalisierung in Staat, Wirtschaft und Gesellschaft, verbunden mit einer immer stärkeren Integration des Internets, einem damit steigenden Vernetzungsgrad und einer Durchdringung mit Informations-und Kommunikationstechnologie (IKT) in nahezu allen Lebensbereichen, entstehen vielfältige neue Anwendungs- und Nutzungsmöglichkeiten für Unternehmen sowie Bürgerinnen und Bürger. Gleichzeitig wächst aber damit auch die Abhängigkeit von IKT in allen Bereichen und damit die Bedeutung der Informationssicherheit (synonym: IT-Sicherheit) hinsichtlich ihrer Schutzgüter Verfügbarkeit, Vertraulichkeit und Integrität. Dass die IT-Sicherheitslage in Deutschland weiterhin angespannt ist, zeigen die Jahresberichte des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) deutlich.

Mit dem vom Bundesinnenminister im Juni des Jahres 2014 angekündigten Entwurf eines IT-Sicherheitsgesetzes plante die Bundesregierung, bestehende Defizite im Bereich der Informationssicherheit – insbesondere bei Betreibern Kritischer Infrastrukturen – abzubauen. Grundsätzlich war das mit dem Gesetzentwurf verfolgte Ziel einer Erhöhung des Niveaus der Informationssicherheit, insbesondere mit Blick auf das Internet und die Kritischen Infrastrukturen, zu begrüßen. Allerdings begegnete der vom Bundesministerium des Innern im August 2014 vorgelegte Referentenentwurf datenschutzrechtlichen Bedenken. Der Name des Gesetzes versprach mehr als sein Inhalt. Auch seitens der Wirtschaft kamen Zweifel auf, ob die geplanten Berichts- und Meldepflichten für Unternehmen, im Ende 2014 vorgelegten Gesetzentwurf des Bundesministerium des Innern, der richtige Weg für einen staatlichen Eingriff zur Informationssicherheit sei.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahm den von der Bundesregierung in das parlamentarische Verfahren eingebrachten Entwurf vom 25. Februar 2015 für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – BT-Drs. 18/4096) zum Anlass, mit einer Entschließung vom 19. März 2015 „IT-Sicherheitsgesetz nicht ohne Datenschutz“ (**Anlage 26**) auf den aus datenschutzrechtlicher Sicht notwendigen Änderungsbedarf hinzuweisen.

Nach Ansicht der Konferenz ist die Informationssicherheit als eine Grundvoraussetzung anzusehen, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren. Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzes kommen.

Die Konferenz wies in ihrer Entschließung besonders darauf hin, dass Maßnahmen zur Erhöhung der Informationssicherheit in den meisten Fällen auch mit einer Verarbeitung personenbezogener Daten verbunden sind. Die damit bestehenden Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Dazu bedarf es klarer gesetzlicher Regelungen, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen.

Zweckbindungsregelungen, betonte die Konferenz, müssen für alle Behörden gelten, die nach dem IT-Sicherheitsgesetz Datenerhebungs- und Datenverarbeitungsbefugnisse erhalten würden. Im Gesetzentwurf war dies nur für das BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes und die Betreiber Kritischer Infrastrukturen vorgesehen. Im Zusammenhang mit den Maßnahmen zur Verbesserung der Informationssicherheit bedarf es zudem gesetzlicher Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschottung.

Auch müssen die Datenschutzaufsichtsbehörden an der Festlegung von Informationssicherheitsstandards beteiligt und in die Informationswege bei der Meldung von IT-Sicherheitsvorfällen mit einbezogen werden, zumal diese häufig auch mit Datenschutzpannen verbunden sein werden.

Nach sechsmonatiger parlamentarischer Beratung und nachdem auch der Bundesrat am 10. Juli 2015 den Gesetzentwurf der Bunderegierung passieren ließ (BR-Drs. 284/15 (Beschluss)), trat das IT-Sicherheitsgesetz vom 17. Juli 2015 (BGBl. I S. 1324) am 25. Juli 2015 in Kraft. Die Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden nur zum Teil vom Gesetzgeber berücksichtigt.

Abschließend ist darauf hinzuweisen, dass die Bestrebungen nach mehr Informationssicherheit sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken dürfen. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

Besonders zum Thema **Verschlüsselung** hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit ihrer Entschließung vom 28. März 2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ (**Anlage 6**) auf die Notwendigkeit des aktiven Handels von Politik und Wirtschaft aufmerksam gemacht und gleichzeitig dazu einen Forderungskatalog aufgestellt:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,

11. Sensibilisierung von Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat hierzu einen Maßnahmenkatalog formuliert, der die genannten Forderungen konkretisiert (**Anlage 7**).

Leider haben diese Forderungen keine Berücksichtigung im IT-Sicherheitsgesetz gefunden. Der Landesbeauftragte erinnert in diesem Zusammenhang an die Digitale Agenda 2014-2017 der Bundesregierung vom August 2014: Die Bundesregierung hat in ihren eigenen Zielstellungen deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist: *„Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden.“*

Daran wird sich die Bundesregierung messen lassen müssen, wenn es gilt, unter dem Thema „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft“ wirksame und vor allem nutzbare Verschlüsselungsmethoden für Unternehmen sowie Bürgerinnen und Bürger umfassend in die Praxis umzusetzen. Das Thema Verschlüsselung und die dazu erhobenen Forderungen der Datenschutzbeauftragten des Bundes und der Länder (vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015, **Anlage 27**) bleiben aktuell. Auch die Landesregierung muss hier aktiv werden (siehe auch Nr. 4.5).

4.5 Vertrauliche Kommunikation im Landesnetz – Fehlanzeige

Als Reaktion auf die Enthüllungen des Whistleblowers Edward Snowden brachte die Fraktion DIE LINKE einen Antrag „Vertrauliche Kommunikation fördern“ vom 7. Oktober 2014 (LT-Drs. 6/3485) in den Landtag ein. Dem Antrag nach sollte sich der Landtag zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und Länder zur „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ (**Anlage 6**) vollumfänglich bekennen (vgl. Nr. 4.4). Dazu sollte den Ministerien die Möglichkeit gegeben werden, den Bürgern eine Ende-zu-Ende-Verschlüsselung anzubieten und eine Überprüfung der bestehenden „Public Key Infrastructure Land Sachsen-Anhalt“ (PKI-LSA) hinsichtlich ihrer Leistungsfähigkeit erfolgen, um diese ggf. durch finanzielle und personelle Unterstützung aufzuwerten.

Der daraufhin von den Koalitionsfraktionen von CDU und SPD am 15. Oktober 2014 gemeinsam eingereichte Änderungsantrag (LT-Drs 6/3513) änderte den Beschlussantrag der Fraktion DIE LINKE dahingehend ab, dass die Entschließung der Datenschutzkonferenz nur noch begrüßt und die Möglichkeit der Ende-zu-Ende-Verschlüsselung zwischen Ministerien und Bürger lediglich geprüft werden solle. Die Möglichkeit der Aufwertung der PKI-LSA wurde im Änderungsantrag getilgt. Mit diesem Antrag waren damit keine weiteren Konsequenzen für ein konkretes Handeln der Landesregierung verbunden. In beiden Anträgen wurde allerdings darum geworben, auf den Webseiten des Landesportals unter www.sachsen-anhalt.de stets gut sichtbar und zugänglich Informationen zur verschlüsselten Kommunikation anzubieten. Ferner wurde in beiden Anträgen die Landesregierung gebeten, im Bundesrat darauf hinzuwirken, die vertrauliche Kommunikation mittels Ende-zu-Ende-Verschlüsselung im E-Government-Gesetz des Bundes auszugestalten. Der Landtag fasste am 17. Oktober 2014 zur LT-Drs. 6/3485 auf der Basis des Änderungsantra-

ges einen Beschluss (LT-Drs. 6/3532), der zumindest die Grundforderungen der Entschließung der Datenschutzkonferenz unterstützte.

In ihrem Bericht (LT-Drs. 6/3734) zur Realisierung des Beschlusses des Landtages informierte die Landesregierung über ihre geplanten Maßnahmen. Unter anderem sollten auf den Webseiten der Ministerien und Kampagnen des Landes auf geeignete Art und Weise Informationen zur verschlüsselten Kommunikation im Internet angeboten werden. Weiterhin sollte geprüft werden, inwieweit sichere Übertragungswege für Informationen vorgesehen werden können und das im Rahmen von Öffentlichkeitsarbeit über die Nutzung von Verschlüsselungsmethoden in der Netzkommunikation informiert werde. Abschließend teilte die Landesregierung in ihrem Bericht mit, dass von ihr das Thema Ende-zu-Ende-Verschlüsselung im Rahmen des E-Government-Gesetzes des Bundes im IT-Planungsrat zur Diskussion gestellt werde.

Der Antwort der Landesregierung vom 11. August 2015 (LT-Drs. 6/4299) auf eine Kleine Anfrage (KA 6/8839) zur Umsetzung der Beschlussrealisierung zur vertraulichen Kommunikation ist zu entnehmen, dass die Landesregierung nach fast acht Monaten noch keinerlei Maßnahmen zur Umsetzung der vertraulichen Kommunikation ergriffen hat. Der aktuelle Arbeitsstand besteht immer noch überwiegend im Prüfen möglicher Lösungen. Auf den Seiten des Landesportales sind Hinweise zur Möglichkeit der vertraulichen Kontaktaufnahme mit den Landesbehörden nur beim Landesbeauftragten für den Datenschutz zu finden. Bei den übrigen Landesbehörden, insbesondere den Ministerien, sucht der Bürger vergebens nach Informationen zur Verschlüsselung von E-Mails und entsprechenden öffentlichen Schlüsseln, mittels derer er eine verschlüsselte Kommunikation mit Landesbehörden aufnehmen könnte. Ganz im Gegenteil, das stets gut sichtbare und zugängliche Kontaktformular des Landesportals weist explizit darauf hin, dass keine verschlüsselte und/oder signierte Kommunikation möglich sei.

Im Rahmen der Initiative „E-Mail made in Germany“ warben namhafte Internetprovider damit, dass Sie auf Ihren E-Mail-Servern zumindest eine durchgängige Transportverschlüsselung bei der E-Mail-Übertragung untereinander etabliert haben (vgl. Nr. 5.1). Grundsätzlich war diese Initiative zu begrüßen. Angesichts des Ausmaßes der Spähattacken durch die NSA kam jedoch die Frage auf, warum das seit 1994 verfügbare Protokoll nicht schon eher zum Einsatz gekommen ist. Auf Anfrage beim zuständigen Ministerium der Finanzen, ob der Einsatz einer durchgängigen Transportverschlüsslung auf den E-Mail-Servern des Landes Sachsen-Anhalt zeitnah umgesetzt werden würde, wurde dem Landesbeauftragten mitgeteilt, dass eine Umsetzung derzeit nicht geplant sei, da weder die personellen noch die finanziellen Kapazitäten zur Umstellung der drei Landes-E-Mail-Server auf das TLS-Protokoll vorhanden wären. Eine etwaige Umstellung sei mit der Einführung des neuen Landesnetzes ITN-XT im Jahre 2018 denkbar. Der Ist-Zustand, dass die E-Mail-Server des Landes transportverschlüsselte Übertragungen nicht entgegennehmen und damit vom Sender den unverschlüsselten Versand erzwingen, wird also noch für mindestens drei weitere Jahre erhalten bleiben. Auch der E-Mail-Transport im Landesnetz wird nicht vor dem Zugriff Unbefugter innerhalb des Landesnetzes geschützt. Ob sich die Landesbehörden beim täglichen Arbeiten und Austauschen von elektronischen Dokumenten dessen bewusst sind, ist fraglich.

Da eine Transportverschlüsselung zeitnah nicht geplant ist, bliebe Bürgern und Behörden, die gewillt sind, vertraulich elektronisch zu kommunizieren, nur noch die

Durchführung einer Ende-zu-Ende-Verschlüsselung beim Versenden von E-Mails übrig. Dies wird jedoch durch die wenig praktikable Umsetzung der PKI-LSA behindert. Die Zertifizierungsstellen (sog. Certificate Authority) der PKI-LSA sind im öffentlichen Internet nicht bekannt. Sie werden auch nicht in Betriebssystemen oder E-Mail-Clients als vertrauenswürdige Zertifizierungsstellen geführt. Das heißt, die Zertifikate der Aussteller der Landes-Zertifikate sind technisch gesehen unbekannt. Wenn allerdings der Aussteller eines Zertifikates unbekannt ist, wird auch dem Zertifikat nicht vertraut und es kann in den meisten Anwendungen nicht genutzt werden. Somit bliebe es dem Bürger sogar dann versagt, eine vertrauliche elektronische Kommunikation herzustellen, wenn Behörden ihren öffentlichen Schlüssel aus der PKI-LSA zur E-Mail-Verschlüsselung anbieten würden. Zurzeit bietet kein Ministerium öffentliche Schlüssel zur vertraulichen elektronischen Kontaktaufnahme an. Weder X.509-Zertifikate aus der PKI-LSA noch selbsterstellte OpenPGP-Schlüssel werden so, wie auf den Webseiten des Landesbeauftragten[3], öffentlich zur Verfügung gestellt. Momentan wird also weder eine mit geringem Aufwand zu implementierende Transportverschlüsselung mittels TLS noch eine zertifikatbasierte Ende-zu-Ende-Verschlüsselung durch die Landesregierung zur Verfügung gestellt. Diese Verfahren werden jedoch spätestens bei Einführung des elektronischen Rechtsverkehrs von großer Bedeutung sein.

Gemäß dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) ist der elektronische Zugang zur Justiz ab dem 1. Januar 2018 zu allen deutschen Gerichten zu ermöglichen (vgl. Art. 24 und 26). Das Gesetz erlaubt den Landesjustizverwaltungen jedoch, den elektronischen Zugang zur Justiz bis zum 31. Dezember 2019 zu verschieben. Nach dem Gesetzeswortlaut kann diese Entscheidung jedoch nur von allen Ländern gemeinsam getroffen werden. Deshalb ist momentan nicht davon auszugehen, dass ein späterer Zeitpunkt entscheidend sein wird.

Spätestens ab 1. Januar 2022 wird die elektronische Einreichung von Schriftsätzen und Anlagen für die Anwaltschaft und auch die Behörden verpflichtend. Die Einreichung in Papierform wird unzulässig. Von dieser Verpflichtung ausgenommen sind Urkunden in Urkundsverfahren. Das Gesetz sieht vor, dass jede Landesjustizverwaltung den verpflichtenden Elektronischen Rechtsverkehr (ERV) separat auf den 1. Januar 2020 oder auf den 1. Januar 2021 vorverlegen kann.

Sofern die Landesregierung nicht von der Möglichkeit Gebrauch macht, die Einführung des verpflichtenden ERV vorzuverlegen, wird die Einführung des verpflichtenden Elektronischen Rechtsverkehrs zum 1. Januar 2022 erfolgen. Eine derart weitreichende und komplexe Infrastruktur sollte weit im Vorfeld dieses Termins vorbereitet werden. Es müssen nicht nur die entsprechenden finanziellen Mittel eingeplant werden, sondern die Basisinfrastruktur (ab 2018, ITN-XT) und die Basisdienste (E-Mail und Internet) müssen bereit sein für die zusätzlichen Anforderungen. Außerdem muss innerhalb der Landesbehörden Expertise zum Thema Verschlüsselung aufgebaut werden.

Angesichts der absehbaren Einführung des ERV ist es nicht verständlich, warum die Landesregierung das Thema Verschlüsselung so vehement ignoriert und Entschei-

[3] http://lsaurl.de/HinweiseEMail

dungen dazu fortlaufend hinausschiebt. Offensichtlich ist die Landesregierung bislang nicht gewillt, Jahrzehnte alte Mindeststandards bei der vertraulichen Kommunikation, wie HTTPS und TLS, zu implementieren. So ist in absehbarer Zeit die Gewährleistung von Vertraulichkeit weder im Landesportal noch auf den zentralen E-Mail-Servern des Landes mittels Verwendung von Transportverschlüsselung geschweige denn durch den Einsatz von Ende-zu-Ende-Verschlüsselung vorgesehen. Der Landesbeauftragte wird sich trotzdem weiterhin engagiert für die Gewährleistung von Vertraulichkeit bei der elektronischen Kommunikation mit Landesbehörden einsetzen, u. a. als Mitglied des Strategiegremiums zum Projekt „Einführung des elektronischen Rechtsverkehrs (ERV) in der Justiz des Landes Sachsen-Anhalt“ (siehe Nr. 7.4).

4.6 Zentraler IT-Dienstleister für Sachsen-Anhalt – Dataport

Mit dem Inkrafttreten des Staatsvertrages über den Beitritt des Landes Sachsen-Anhalt zum IT-Verbund der nordostdeutschen Länder – Dataport vom 13. Dezember 2013 (GVBl. LSA S. 524) am 24. Februar 2014 (GVBl. LSA S. 94) begann für das Land gemäß dieser grundlegenden strategischen Entscheidung eine neue Etappe bei der Konsolidierung der IT-Landschaft der Landesverwaltung. Ziel dieses Beitritts ist es, langfristig die Modernisierung der Landesverwaltung durch die Nutzung gemeinsamer Rechenzentren, IT-Infrastrukturen und -Verfahren in den sechs Trägerländern sicherzustellen sowie die damit verbundenen Synernergieeffekte beim Einsatz moderner Informations- und Kommunikationstechnologien (IKT) zu nutzen. Wie der Landesbeauftragte bereits in seinem XI. Tätigkeitsbericht (Nr. 4.4) beschrieben hatte, ist es nunmehr seit 1991 der 4. Versuch einer Landesregierung, die Konsolidierung der IKT der Landesverwaltung und die Konzentration von Querschnittsdiensten mit Hilfe eines zentralen IT-Dienstleisters für die Landesverwaltung zu erreichen. Mit Art. 2 des Zustimmungsgesetzes zum Staatsvertrag wurde gleichzeitig die Eingliederung des bisherigen Landesrechenzentrums (Abteilung 4 der Oberfinanzdirektion Magdeburg) zum 1. Januar 2014 in Dataport beschlossen. Der Landesbeauftragte hatte die Möglichkeit, zum Entwurf des Zustimmungsgesetzes zum Staatsvertrag im August 2013 Stellung zu nehmen. Durch den Beauftragten der Landesregierung für Informationstechnik (CIO) des Ministeriums für Finanzen wurde in der Folge dem Landesbeauftragten eine Übersicht von 125 Fachverfahren der Ressorts zur Verfügung stellt, die bisher vom Landesrechenzentrum betrieben wurden und deren endgültige Migration zu Dataport für das Jahr 2016 prognostiziert wurde.

Als erstes Verfahren wurde im März 2014 das Besteuerungsverfahren übergeleitet. Der Landesbeauftragte hatte dabei die Auftraggeberstelle Steuern des Ministeriums der Finanzen, als verantwortliche Stelle für alle Steuerfachverfahren, beratend unterstützt und dabei die Erstellung der notwendigen Verfahrensverzeichnisse für die migrierten Steuerfachverfahren angemahnt. Eine weitere Information über den Verlauf dieser Migration und die erarbeiteten Verfahrensverzeichnisse ist bisher ausgeblieben. Die mit dem Landesbeauftragten abgestimmte Rahmenvereinbarung zum Datenschutz bei der Verarbeitung personenbezogener Daten von Behörden des Landes Sachsen-Anhalt durch Dataport vom 15. August 2013 ist hier nicht ausreichend.

Zu den Trägerländern von Dataport gehört nunmehr neben Schleswig-Holstein, Hamburg, Bremen, Niedersachsen und Mecklenburg-Vorpommern auch Sachsen-Anhalt. Dataport führt insbesondere *Auftragsdatenverarbeitungen* durch, wobei die

verschiedenen Datenschutzregeln der jeweiligen Länder zu beachten sind, d. h. das für die Auftraggeber jeweils geltende Recht, für Sachsen-Anhalt ist das § 8 DSG LSA. Bei der Datenverarbeitung im Auftrag für die jeweiligen Trägerländer oder deren Kommunen muss Dataport für einzelne Verfahren zum Teil verschiedene datenschutzrechtliche Regelungen beachten und wird dabei auch von den sechs Datenschutzbeauftragten der Trägerländer kontrolliert. Für den Landesbeauftragten ergeben sich seine Kontrollrechte aus § 15 Abs. 2d und 5 des Staatsvertrages.

Erklärtes Ziel der Gründung von Dataport war, durch Zusammenarbeit der Trägerländer Synergieeffekte zu nutzen. Dies gelingt umso mehr, je mehr Verfahren Dataport länderübergreifend oder zumindest möglichst mit einheitlicher Software zum Einsatz bringen kann. Bei der länderübergreifenden Zusammenarbeit bilden die jeweiligen landesrechtlichen Regelungen die Grenzen. Im technischen und organisatorischen Bereich sind die gesetzlichen Regelungen zur Datensicherheit im Wesentlichen identisch. Unterschiede gibt es im materiellen Recht der Länder. Setzen die Länder Bundesrecht um, z. B. im Bereich des Pass- und Personenstandswesens oder des Meldewesens, sind die Rechtsgrundlagen identisch.

Dataport muss als zentraler Dienstleister für Länder insbesondere bei dem Einsatz von länderübergreifenden Verfahren die *Mandantenfähigkeit* für die einzelnen Länder gewährleisten. Das Thema der Mandantentrennung bei der automatisierten Verarbeitung personenbezogener Daten der einzelnen Länder, insbesondere im neuen Rechenzentrum (RZ²), wird die Landesbeauftragten in Zukunft verstärkt beschäftigen. Da bis zu sechs Landesbeauftragte für Dataport zuständig sind, ist eine Abstimmung u. a. bei den Prüfungsmaßstäben, dem Zusammenwirken bei Prüfungen und bei der Beratung erforderlich. Zur Umsetzung dieser Aufgaben gibt es regelmäßige Treffen der Landesbeauftragten auf Arbeits- und Leitungsebene, um das gemeinsame Zusammenwirken effizienter zu gestalten und ein abgestimmtes Meinungsbild bei datenschutzrechtlichen Fragestellungen im rechtlichen wie im technischen Bereich zu erreichen.

Unabhängig von der Eigenschaft als Trägerland und einer Beauftragung von Dataport als dem zentralen IT-Dienstleister für die Landesverwaltung bleiben die Ressorts bzw. die beauftragenden Behörden *verantwortliche Stelle* gem. § 2 Abs. 8 DSG LSA. Aus diesem Grunde haben die Ressorts die rechtlichen Voraussetzungen für eine Beauftragung von Dataport für jedes zu migrierende Fachverfahren zu prüfen. Gleiches gilt für ihre Verantwortung als Auftraggeber zur Umsetzung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit gem. § 6 Abs. 2 und 3 DSG LSA.

Besondere Beachtung muss bei der Auftragsvergabe durch die Ressorts an Dataport dem novellierten Datenschutzgesetz vom 21. Juli 2015 (GVBl. LSA S. 365) und hier insbesondere den Regelungen zur *Auftragsdatenverarbeitung* (§ 8 Abs. 2) geschenkt werden. Den Abschluss von EVB-IT-Verträgen bei der Migration von Fachverfahren der Ressorts zu Dataport hält der Landesbeauftragte deshalb für nicht ausreichend. In ihrer Datenschutz-Leitlinie vom 2. September 2015 verpflichtet sich Dataport, den Auftraggebern (Kunden) die notwendige Unterstützung bei der Erstellung eines Sicherheitskonzeptes zu geben. Weiterhin verpflichtet sich Dataport, für jedes im Auftrag betriebene automatisierte Verfahren die für das *Verfahrensverzeichnis* erforderlichen Informationen zur Verfügung zu stellen. Hier hat Dataport gegenüber seinen Auftraggebern eine Bringschuld.

Für eine umfassende Beachtung des Datenschutzes und der Datensicherheit sollten Dataport und seine Auftraggeber seitens der Trägerländer die Datenschutzbeauftragten rechtzeitig bereits im Planungsstadium über automatisierte Vorhaben und Verfahren bzw. deren wesentliche Änderung informieren und beteiligen, so wie es z. B. auch § 14 Abs. 1 Satz 2 DSG LSA vorschreibt.

4.7 Bring Your Own Device – Umsetzung bei Dataport

In seinem XI. Tätigkeitsbericht (Nr. 4.9) formulierte der Landesbeauftragte Anforderungen an den Einsatz von „Bring Your Own Device“ (BYOD) in Behörden und Unternehmen. BYOD bezeichnet ein Nutzungskonzept, bei dem Beschäftigte in Absprache mit dem Arbeitgeber ihre privaten mobilen Endgeräte (Smartphones, Tablets, Notebooks) zur Durchführung ihrer beruflichen Tätigkeiten verwenden dürfen oder sollen. Der zentrale IT-Dienstleister des Landes Sachsen-Anhalt Dataport plant für die Umsetzung von BYOD den Einsatz der verschlüsselten Container-Lösung Dynamic Mobile Exchange™ (DME™) der dänischen Firma Excitor.

Der Zugang zu Servern und Diensten des Landesnetzes würde in Zukunft für Smartphones und Tablets wie schon bei Notebooks und Heimarbeitsplätzen per VPN-Tunnel auf Citrix-Umgebungen erfolgen. Dabei kann die Anmeldung innerhalb der Citrix-Umgebung via Active Directory im Landesnetz durchgeführt werden. Da mobile Endgeräte nicht immer online sind, muss parallel dazu eine Lösung für den Einsatz offline umgesetzt werden. Die Clientkomponente von DME™ wird dabei zunächst als App auf dem mobilen Endgerät installiert. Die zentrale Serverkomponente wird durch Dataport innerhalb des Landesnetzes betrieben und mit einer öffentlichen IP-Adresse im Internet bereitgestellt. Die Konnektoren, auf die der Server zurückgreift, werden in den Ressorts angesiedelt sein. Sie stellen die Verbindung zu den hiesigen Diensten und Daten her. Client und Server können über eine zertifikatsbasierte verschlüsselte Verbindung miteinander kommunizieren. Die Firma Excitor nennt dies Micro-VPN. Dadurch können in der DME™-App Exchange-Postfächer, freigegebene Dateien sowie Extranet- und Intranet-Webseiten des Landesnetzes abgerufen werden. Innerhalb der App existieren Programme wie E-Mail-Client oder Adressbuch, die eine entsprechende Handhabbarkeit gewährleisten, ohne dabei auf Apps aus dem privaten unverschlüsselten Bereich des mobilen Endgerätes zurückzugreifen. Die lokal anfallenden Daten, wie E-Mail-Anhänge, werden von DME™ in einem AES-verschlüsselten Container auf dem mobilen Endgerät abgelegt. Ein Zugriff durch private Apps oder systeminterne Prozesse wird dadurch ausgeschlossen. Gleichwohl ermöglicht es die App, lokale Daten, z. B. Kontaktdaten, aus dem verschlüsselten Container in den unverschlüsselten privaten Bereich zu synchronisieren.

Grundsätzlich sind die Bemühungen von Dataport, eine sichere und datenschutzgerechte Lösung für BYOD im Land Sachsen-Anhalt bereitzustellen, zu begrüßen. Zurzeit liegen allerdings noch zu wenige Informationen über die Umsetzung mit Excitor DME™ vor, um eine abschließende Beurteilung vornehmen zu können. Vorab lässt sich jedoch darauf hinweisen, dass beim Einsatz von DME™ verhindert werden sollte, dass im Container verschlüsselte dienstliche Daten, wie das Adressbuch, in den privaten Bereich des Gerätes synchronisiert werden. Denn in dienstlichen Dokumenten oder im dienstlichen Adressbuch befinden sich ggf. personenbezogene Daten, die in dieser Form nicht öffentlich zugänglich sind. Das private Dateisystem bzw. Ad-

ressbuch des mobilen Endgerätes ist jedoch unter Umständen für andere Apps freigegeben und könnte somit ungewollt bzw. unbewusst in eine Cloud synchronisiert oder an Dritte übermittelt werden. Des Weiteren würden die in den privaten Bereich synchronisierten Daten einer Fernlöschung, die bei Verlust des Gerätes innerhalb des DME™-Containers möglich ist, entzogen werden. Außerdem muss dafür Sorge getragen werden, dass auch Privatgeräte regelmäßig mit Sicherheitsupdates versorgt und durch Virenschutzprogramme überprüft werden. Dies könnte zu einer enormen Herausforderung für die lokalen IT-Administratoren in den Ressorts werden.

4.8 Sicherheitsrisiko Heartbleed und Co.

Gemäß Satz 2 Nr. 4 der Anlage zu § 9 Satz 1 BDSG hat eine verantwortliche Stelle, die personenbezogene Daten automatisiert verarbeitet, u. a. zu gewährleisten, dass diese Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen oder kopiert werden können (Weitergabekontrolle). Analog dazu haben Behörden des Landes Sachsen-Anhalt gemäß § 6 Abs. 2 Satz 1 Nr. 1 DSG LSA zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit).

„Heartbleed“ (CVE-2014-0160; engl. für „Herzbluten“), eine im April 2014 bekannt gewordene Sicherheitslücke der Heartbeat-Erweiterung (engl. für „Herzschlag“) von OpenSSL in der Version 1.0.1 bis 1.0.1f. OpenSSL ist eine freie Software-Bibliothek zur Umsetzung von Transport Layer Security (TLS), also Transportverschlüsselung des Datenverkehrs im Internet. Die Heartbeat-Erweiterung ermöglicht es Kommunikationspartnern einer transportverschlüsselten Verbindung, durch fortlaufendes Versenden von Nachrichten überprüfen zu können, dass die Verbindung zueinander noch besteht. Dabei sendet der Empfänger die Inhalte einer Nachricht zurück an den Sender. Der Fehler in der Implementierung besteht darin, dass beim Zurücksenden einer Nachricht nicht die Länge der ursprünglichen Nachricht überprüft wird. So ist es möglich, dass ein Sender seiner Gegenstelle eine kurze Nachricht übersendet, ihr jedoch mitteilt, dass die Nachricht viel länger ist. Die Gegenstelle liefert dann eine Nachricht zurück, die die ihr mitgeteilte Länge hat. Da der ursprüngliche Nachrichteninhalt kürzer ist als die zurückgesendete Nachricht, wird der Rest der zurückgesendeten Nachricht mit Inhalten aus dem flüchtigen Speicher (Memory) der Gegenstelle aufgefüllt. Im flüchtigen Speicher eines Servers befinden sich alle Daten, die der Server gerade verarbeitet, so auch personenbezogene Daten, die eingegeben oder abgerufen werden, Logindaten, Kennwörter oder Schlüssel einer verschlüsselten Kommunikation. Somit ist es Angreifern möglich, durch gezieltes Absenden manipulierter Heartbeat-Nachrichten nach und nach den flüchtigen Speicher eines Servers auszulesen.

Werden von einem Server, der diese Sicherheitslücke besitzt, personenbezogene Daten über das Internet übertragen, kann eine Weitergabekontrolle im Sinne der Anlage zu § 9 Satz 1 BDSG nicht gewährleistet werden. Ferner ist davon auszugehen, dass die privaten Schlüssel bzw. Serverzertifikate, die genutzt werden, um die Kommunikation mit dem Server zu verschlüsseln, durch die Sicherheitslücke kompromittiert worden sind. Da die Sicherheitslücke bereits seit März 2012 besteht, kann ein Serverbetreiber, der personenbezogene Daten mit Hilfe einer verschlüsselten Verbindung zum Server erhebt oder verarbeitet, selbst nach Schließung der Sicherheits-

lücke die Weitergabekontrolle im Sinne der Anlage zu § 9 BDSG nicht gewährleisten, wenn er nach Schließen der Sicherheitslücke nicht auch geheime Schlüssel bzw. Serverzertifikate erneuert. Werden personenbezogene Daten über verschlüsselte kennwortgeschützte Zugänge übertragen, so sollten außerdem die Kennwörter erneuert werden, da aufgrund der Kompromittierung des Verschlüsselungsverfahrens potentiell davon ausgegangen werden kann, dass auch die Kennwörter Unbefugten zur Kenntnis gelangt sein können.

Nach Heartbleed sind weitere gravierende Sicherheitslücken im Umfeld von unter Linux betriebenen Webservern bekannt geworden, die es ermöglichen können, unbefugt personenbezogene Daten aus Onlinediensten abzufangen. Es ist dringend angeraten, die Sicherheitslücken schnellstmöglich zu schließen, falls noch nicht geschehen.

Padding Oracle On Downgraded Legacy Encryption (Poodle) (CVE-2014-3566) ist im Mai 2014 bekannt geworden und basiert auf der Ausnutzung einer Sicherheitslücke einer Vorgängerversion des Transportverschlüsselungsprotokolls Transport Layer Security (TLS) der aktuellen Version 1.2. Dabei wird per Man-In-The-Middle-Attack der Datenverkehr so manipuliert, dass der Client dem Server mitteilt, er unterstütze die aktuelle Version des TLS-Protokolls nicht. Der Server wechselt dann automatisch auf eine Vorgängerversion des Protokolls, um die Kommunikation doch noch verschlüsseln zu können. Greift der Server hierbei auf das Secure-Sockets-Layer-Protokoll (SSL) der Version 3.0 zurück, kann eine Sicherheitslücke in diesem veralteten Protokoll, namens Padding-Oracle-Attacke, ausgenutzt werden. Die Sicherheitslücke lässt sich schließen, indem die Unterstützung des SSL-Protokolls der Version 3.0 und älter auf den Servern deaktiviert wird. Die Verwendung des veralteten SSL-Protokolls kann auch clientseitig in den meisten Webbrowsern deaktiviert werden.

Bei Shellshock (CVE-2014-6271) handelt es sich um eine im September 2014 bekannt gewordene Sicherheitslücke der von allen Linux-Systemen verwandten Kommandozeile „Bash“ in den Versionen 1.03 bis 4.3. Hierbei ist es möglich, ausführbaren Code in Form von Umgebungsvariablen an die Bash zu übergeben. Dies kann z. B. bei Ausführung von Skripten des Common Gateway Interface (CGI) in Webseiten ausgenutzt werden, da die Ausführung des Skriptcodes bei CGI vom Webserver an die Kommandozeile des darunterliegenden Betriebssystems übergeben wird. Somit kann per CGI eingeschleuster Schadcode als Umgebungsvariable in die Bash geladen und dort auf Betriebssystemebene ausgeführt werden. Die Schließung der Sicherheitslücke erfolgt über ein Update der Bash.

Abschließend muss betont werden, dass es immer wieder Sicherheitslücken in offener freier Software geben wird, die erst lange Zeit nach ihrem ersten Auftreten bekannt werden und somit geschlossen werden können. Daher liegt es in der Verantwortung einer jeden Behörde und eines jeden Unternehmens, die bzw. das personenbezogene Daten verarbeitet, regelmäßig und fortlaufend aktuelle Bedrohungen durch die IT-Abteilungen identifizieren und neutralisieren zu lassen, um so den Forderungen des § 6 DSG LSA nach Vertraulichkeit und der Anlagen zu § 9 BDSG nach Weitergabekontrolle gerecht werden zu können. Aktuelle sowie ältere Sicherheitslücken aller Art können z. B. im Archiv des Portals des Computer Emergency Respon-

se Teams (CERT) des Deutschen Forschungsnetzes (DFN) im Internet[4] abgerufen werden.

4.9 Umgang mit Spam-Mails

Das E-Mail-Protokoll SMTP verfügt in seiner Grundform nicht über Mechanismen, die einen E-Mail-Absender authentifizieren. Aus diesem Grund kann ein entsprechend modifizierter Mailserver eine E-Mail mit einer beliebigen existierenden oder nicht existierenden Absender-Adresse versenden. Sofern E-Mails nicht vom Absender digital signiert sind, kann nicht ermittelt werden, von welchem Absender eine E-Mail tatsächlich stammt. Teilweise werden zur Versendung von Spam-Mails infiltrierte Rechner von Firmen oder Privatpersonen in Mailserver umgewandelt, ohne dass die Besitzer etwas davon erfahren. Das heißt, weder die E-Mail-Adresse des Absenders noch die Serveradresse, von der die E-Mail übermittelt wurde, lassen Rückschlüsse darauf zu, woher eine E-Mail tatsächlich stammt.

Dass die eigene E-Mail-Adresse in die Hände von Spam-Versendern gerät, kann verschiedene Ursachen haben:

Zum einen können Empfängeradressen schlichtweg geraten werden. Ein Computerprogramm kann mühelos sekundenschnell hunderte zufällige E-Mail-Adressen aus den Buchstaben des Alphabets, den zehn Ziffern und den Sonderzeichen "." und "@" bilden und sofort versenden. Bei falsch geratenen Adressen erhält der Mailserver eine Unzustellbarkeitsnachricht. Bei richtig geratenen E-Mail-Adressen geschieht dies nicht, wenn die E-Mail zugestellt werden konnte. Dadurch wird dem Spam-Versender bekannt, welche der geratenen E-Mail-Adressen tatsächlich existieren. Die auf diesem Wege ermittelten realen E-Mail-Adressen werden unter Spam-Versendern ausgetauscht. Somit können die Adresslisten der Spam-Versender immer größer werden, ohne dass eine einzige E-Mail-Adresse über eine Datenerhebung ermittelt werden musste.

Zum anderen können über Schadsoftware infiltrierte Rechner den Datenverkehr benachbarter Rechner im Netzwerk beobachten und aus den unverschlüsselten Verkehrsdaten E-Mail-Adressen herausfiltern. So kann z. B. in einem öffentlich freigegebenen WLAN der unverschlüsselte E-Mail-Verkehr oder Loginversuche beim Provider problemlos mitgelesen werden. Die infiltrierten Rechner sammeln diese E-Mail-Adressen und senden sie weiter an den Urheber der Schadsoftware (Spyware). Urheber von Spyware und Trojanern können neben staatlichen Geheimdiensten auch Netzwerke von kriminellen Programmierern sein, die unerkannt an personenbezogene Daten gelangen wollen, um daraus Profit zu schlagen.

Des Weiteren ist es möglich, dass personenbezogene Daten infolge von Sicherheitslücken bei Unternehmen „gestohlen“ werden. Die verantwortlichen Stellen in Deutschland sind in den Fällen des § 42a BDSG dazu verpflichtet, derlei Datenpannen der zuständigen Aufsichtsbehörde zu melden, wenn schwerwiegende Beeinträchtigungen zu befürchten sind (siehe Nr. 14.3).

[4] https://portal.cert.dfn.de/adv/archive/

Da eine unverschlüsselte und unsignierte E-Mail häufig nicht vertrauenswürdig ist, sollten über diesen frei zugänglichen ungesicherten Dienst keine personenbezogenen Daten kommuniziert werden. Im Zweifelsfall sollte eine E-Mail hinterfragt und fernmündlich oder postalisch beim tatsächlichen (Vertrags-)Partner Rücksprache gehalten werden.

Ein Missbrauch der eigenen E-Mail-Adresse lässt sich nach aktuellen Kenntnissen nicht mit Sicherheit vermeiden. Die verantwortlichen Stellen, die von den Spam-Versendern als Absender missbraucht werden, sind im gleichen Maße Opfer wie die Spam-Empfänger[5]. Als praktischer Rat kann allerdings empfohlen werden, die Filtermöglichkeiten des Spam-Schutzes sowohl vom E-Mail-Provider als auch vom eigenen E-Mail-Programm in vollem Umfang zu nutzen. Viele E-Mail-Provider bieten einen Spam-Schutz an, der jedoch erst in den Einstellungen aktiviert werden muss. E-Mail-Clients mit eingebauten lernfähigen Spam-Filtern sind im Internet kostenfrei erhältlich.

Die für die Erhebung einer E-Mail-Adresse und anschließenden Versendung von Spam-Mails verantwortliche Stelle lässt sich aus technischen Gründen nicht ermitteln. Der Landesbeauftragte kann in solchen Fällen nur Maßnahmen veranlassen, wenn Hinweise vorliegen, die auf eine verantwortliche Stelle in Sachsen-Anhalt deuten.

Hinweise zu Spam-Versendern und Autoren von Schadsoftware können über das eRevier[6] dem LKA mitgeteilt werden. Das LKA leitet die Informationen an Stellen des Bundes weiter. Diese können ggf. in Zusammenarbeit mit Interpol und Europol Muster bei den Spam-Versendern erkennen und eventuell die Urheber rechtswidriger E-Mail-Inhalte ermitteln.

4.10 Deep Packet Inspection

In größeren IT-Infrastrukturen werden oft Erkennungssysteme betrieben, die Eindringlinge und schadhafte Programme identifizieren, melden und blockieren können. Dazu wird u. a. der gesamte Netzwerkverkehr überwacht und analysiert. Um die Erkennungsquote dieser Intrusion Detection Systeme (IDS) zu maximieren, kann neben den Metainformationen, wie Kommunikationsprotokoll, Herkunft oder Größe, auch der Inhalt von Datenpaketen im Netzwerk ausgewertet werden. In diesem Fall ist von Deep Packet Inspection (DPI) die Rede. Wird DPI innerhalb von Unternehmensnetzwerken angewendet, müssen u. a. datenschutzrechtliche Aspekte Berücksichtigung finden.

Zunächst muss eine Fallunterscheidung vorgenommen werden. Unternehmen, die die private Nutzung des Internets für Mitarbeiter gestatten, sind Telekommunikationsdiensteanbieter i. S. d. Telekommunikationsgesetzes (TKG). Der Einsatz von DPI bei IDS unterliegt dann den Vorschriften des TKG. Das Bundesdatenschutzgesetz (BDSG) kommt hier subsidiär zur Anwendung.

---

[5] siehe z. B. http://lsaurl.de/GefRech

[6] http://www.polizei-web.sachsen-anhalt.de/erevier/

Gemäß § 100 Abs. 2 Satz 1 TKG darf der Betreiber der Telekommunikationsanlage, soweit erforderlich, zur Erkennung und Eingrenzung von Störungen, worunter auch Angriffe auf die Infrastruktur zu zählen wären, auf bestehende Verbindungen aufschalten. § 100 Abs. 1 TKG stellt klar, dass die Verkehrsdaten der Teilnehmer zu diesem Zweck erhoben und verwendet werden können. Nach § 100 Abs. 2 Satz 2 TKG sind bei der Aufschaltung angefertigte Aufzeichnungen unverzüglich zu löschen.

Somit wäre der Einsatz eines IDS (Erheben von Verkehrsdaten zur Erkennung von Störungen) grundsätzlich unbedenklich. Sollte jedoch im Rahmen der Intrusion Detection DPI (Aufschalten auf bestehende Verbindungen) zur Anwendung kommen, wäre dafür zu sorgen, dass nur erforderliche Daten erhoben und diese nach sofortiger automatisierter Auswertung unverzüglich gelöscht werden. Außerdem dürfen die Daten gemäß § 31 BDSG nur für die o. g. Zwecke erhoben und genutzt werden. Somit wäre nicht zulässig, die Inhalte der Datenpakete zu speichern und den Nutzern der Telekommunikationsanlage zuzuordnen. Die bloße Analyse eines Datenpaketes darauf, ob es Schadprogramme enthält, mit dem Ziel, durch das IDS die Zustellung des Datenpaketes zu verhindern und Alarm auszulösen, wäre grundsätzlich zulässig, wenn dadurch Bedrohungsszenarien verhindert werden können.

Sollte es sich bei einem Unternehmen nicht um einen Anbieter von Telekommunikationsdiensten handeln, wäre ausschließlich das BDSG anzuwenden. In dem Fall ist gemäß § 28 Abs. 1 Nr. 2 BDSG eine Datenerhebung durch DPI zulässig, da sie zur Wahrung berechtigter Interessen, hier Abwehr von Schadprogrammen, durchgeführt wird. Allerdings kann hier nur dann davon ausgegangen werden, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung nicht überwiegt, wenn die Auswertung der Datenpakete automatisiert erfolgt und die Inhalte nicht den Betroffenen zugeordnet werden. Die durch DPI anfallenden Daten unterliegen auch hier gemäß § 31 BDSG einer strengen Zweckbindung und dürfen somit ausschließlich zur Abwehr von Schadprogrammen erhoben und genutzt werden. Gemäß § 20 Abs. 2 Nr. 2 BDSG wären die Daten der DPI unverzüglich zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle nicht mehr erforderlich ist.

In beiden Fällen wäre der Einsatz von DPI bei IDS unter Einschränkungen zulässig. Es muss vor allem darauf geachtet werden, dass die durch DPI erhobenen Daten für keinen anderen Zweck genutzt und im Anschluss gelöscht werden.

4.11 Einsatz von Funkmesszählern durch Vermieter

Der Landesbeauftragte erhielt eine Anfrage zur Zulässigkeit von Funkmesszählern, mit deren Hilfe Heizungs- und Wasserverbrauch von Privatwohnungen an einen Dienstleister zur Nebenkostenabrechnung übertragen werden. Diese Geräte haben für Mieter und Vermieter einen erheblichen Vorteil: es müssen keine Termine zum Betreten der Wohnung vereinbart werden. Mitunter haben Mieter aber Vorbehalte gegen diese Geräte, da sie befürchten, dass nicht nur die erforderlichen Verbrauchswerte an den Vermieter übermittelt werden. Den Einbau dieser Geräte haben Mieter nach aktueller Rechtsprechung gemäß § 4 Abs. 2 Heizkostenverordnung bzw. § 554 Abs. 2 BGB zu dulden (vgl. BGH, Urteil vom 28. September 2011, NJW 2011, 3514 f.). Die Frage, inwieweit mithilfe dieser Geräte Verbrauchswerte gemessen und

an den Vermieter oder seine Beauftragten übermittelt werden dürfen, ist jedoch eine datenschutzrechtliche, die gesondert zu prüfen ist.

Auch Informationen zu Heizungs- und Wasserverbräuchen von Mietern sind personenbezogene Daten, da sie Auskunft über sachliche Verhältnisse von natürlichen Personen geben. Diese Informationen können abhängig von der Häufigkeit der Messungen sehr detailliert und aussagekräftig sein. Sie lassen Rückschlüsse zu auf das generelle Heizungs- bzw. Verbrauchsverhalten, die Anwesenheit und die Nutzung bestimmter Räumlichkeiten. Auch die Erstellung von Nutzungsprofilen erscheint möglich (vgl. LG Dortmund, Urteil vom 28. Oktober 2014, Az. 9 S 1/14, juris). Die Erhebung und Speicherung von Heizungs- und Wasserverbräuchen der Mieter ist daher nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene wirksam eingewilligt hat.

Als Erlaubnisvorschrift kommt hier § 28 Abs. 1 Nr. 1 BDSG in Betracht. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung zulässig, wenn es für die Begründung, Durchführung oder Beendigung des Mietverhältnisses erforderlich ist. Regelmäßig werden die o. g. Verbrauchswerte ermittelt zur Erstellung der jährlichen Nebenkostenabrechnung. Daraus folgt, dass die Verbrauchswerte zu diesem Zweck lediglich einmal jährlich an den Vermieter gemeldet werden dürfen, und zwar nur die jeweiligen Endwerte. Zwischenmeldungen dürften nur selten erforderlich sein, z. B. bei einem Mieterwechsel. Die Übermittlung regelmäßiger Statusinformationen des Gerätes bzw. die Meldung der Betriebsbereitschaft ist demgegenüber datenschutzrechtlich nicht zu beanstanden.

In dem vom Landesbeauftragten zu prüfenden Fall hat der Vermieter zur Erfassung und Auswertung des Heizungs- und Wasserverbrauchs der Mieter eine Firma, die auf Messtechnik und Verbrauchswerterfassung spezialisiert ist, beauftragt. Diese meldet die jeweiligen Verbräuche an den Vermieter, der daraufhin die Nebenkostenabrechnung fertigt. Die Erhebung und Speicherung der Verbrauchswerte verlangt hier zusätzlich, dass zwischen Vermieter und der Firma, die die Messungen durchführt, schriftlich eine Auftragsdatenverarbeitung vereinbart wurde, die insbesondere die in § 11 Abs. 2 BDSG benannten Festlegungen enthalten muss. Letztere darf die Daten dann allerdings nur im Rahmen der Weisungen des Vermieters erheben, verarbeiten und nutzen. Der Vermieter hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Schließlich ist beim Einsatz von Funkmesszählern auch die Datensicherheit zu gewährleisten. Es muss sichergestellt werden, dass die Messdaten nur von Berechtigten ausgelesen und den entsprechenden Mietern zugeordnet werden können. Dies erfordert regelmäßig eine verschlüsselte Übermittlung. Diese ist grundsätzlich auch dann erforderlich, wenn die Daten zunächst vom Heizkostenverteiler auf einen zentralen Datenspeicher in einem Mehrfamilienhaus gesendet und von dort aus zu bestimmten Zeiten – z. B. durch Techniker mit mobilen Endgeräten – abgerufen werden. Beide Datenübertragungen sollten verschlüsselt sein.

Abschließend konnte im Hinblick auf die Anfrage feststellt werden, dass durch die von der beauftragten Firma verwendete Messsensorik und Funktechnik keine anderen als die angegebenen Verbrauchsdaten erhoben, verarbeitet und genutzt wurden.

Zu weiteren datenschutzrechtlichen Fragen des Smart Metering im Zusammenhang mit der Novellierung des Energiewirtschaftsgesetzes und aktuell der Digitalisierung der Energiewende siehe den Beitrag unter Nr. 14.5.

4.12 Umgang mit Smartphones und mobilen Datenträgern in Fundbüros

Immer öfter werden in Fundbüros neben normalen Mobiltelefonen, Digitalkameras, Tablets und Laptops auch Smartphones abgegeben. Fundbüros sind nicht nur Verwahrstellen für Fundsachen, sondern sollten auch aktiv Beteiligte bei der Suche nach dem Eigentümer der jeweiligen Fundsache sein. Holt der Eigentümer die Fundsachen nicht innerhalb von sechs Monaten ab und beansprucht der Finder nicht das Eigentum, so kann das Fundbüro die Fundsache versteigern. Aus datenschutzrechtlicher Sicht kann sich ein solches Versteigern bei den eingangs genannten Fundsachen aber nicht auf deren internen Speicher bzw. externe Speichermedien und die darauf gespeicherten Inhalte beziehen. Im internen Speicher bzw. den externen Speichermedien der Geräte können sich personenbezogene Daten der Eigentümer befinden, angefangen bei privaten Fotos und Videos, Nachrichten, Kontaktdaten und vieles mehr. Anfragen von Gemeinden veranlassen den Landesbeauftragten, Empfehlungen für eine praktische Vorgehensweise zu geben.

Fundsachen nur zu erfassen und zu lagern, ist bei Tablets, Mobiltelefonen, Smartphones und mobilen Datenträgern, die oft ohne besondere äußere Merkmale daher kommen und viele private Daten jeglicher Art enthalten, nicht mehr zeitgemäß. Solche Geräte und Datenträger bedürfen unter Umständen einer inhaltlichen Prüfung bezüglich der gespeicherten personenbezogenen Daten, wenn der Eigentümer nicht anderweitig ausfindig gemacht werden konnte, etwa durch Mitteilung der Seriennummer der SIM-Karte an den Provider, der Eigentümer dieser SIM-Karte ist oder durch Nachfrage bei der Polizei, ob solche Fundsachen als gestohlen gemeldet sind (mittels der Seriennummer – IMEI/MEID). Bei Mobiltelefonen ist es meist möglich, auch im gesperrten Zustand, die IMEI zu ermitteln. Die Hersteller haben die Möglichkeit, den Eigentümer zu ermitteln und zu informieren. Dies ist in der Praxis jedoch bisweilen etwas kompliziert. Auf Antrag können oft zumindest Fundbüros bzw. die Polizei die Kontaktdaten erhalten. Derartige Möglichkeiten sollten vorab gezielt evaluiert und von diesen sollte auch Gebrauch gemacht werden. Umgekehrt wäre ggf. auch eine Unterrichtung der örtlichen Polizeidienststellen über gefundene Objekte sinnvoll.

Bei Einzelgeräten ist eine Inbetriebnahme ohne Weiteres möglich. Hier sollten identifizierende Merkmale gleich notiert werden (Seriennummern, Marke, Typ, Startbilder, Kontaktadressen, Daten des Besitzers), da später ggf. mangels Akku oder Lademöglichkeit ein erneutes Abrufen unnötig erschwert werden könnte. Speziell bei Mobiltelefonen und Smartphones sollten die Mitteilungen auf dem Sperrbildschirm gezielt untersucht und notiert werden. Das Anschließen von solchen Geräten an einfache Hardware wie passende Netzteile, Tastaturen, Monitore oder TV-Geräte stellt kein Problem dar, allerdings sind Verbindungen mit dienstlich genutzten Geräten z. B. via USB, SATA/IDE oder LAN-Anschluss aus Sicherheitsgründen (Schutz vor Schadsoftware) zu untersagen. Hier ist eine Abstimmung über eine sichere Vorgehensweise mit der EDV-Abteilung der Behörde notwendig. Gleiches gilt auch für mobile Datenträger und einzelne PC-Komponenten.

Bei einem Anschluss an dienstlich genutzte Rechner ist in jedem Fall darauf zu achten, dass keine Schäden z. B. durch Viren entstehen können. Da vermeintlich liegengelassene USB-Sticks auch als Angriffsmöglichkeit in Frage kommen, sollte ein nur für diesen Einsatzzweck dezidierter PC ohne Netzwerk-Anschluss, ggf. sogar mit einem von DVD bootbaren Live-Betriebssystem, genutzt werden.

Für eine komplette Löschung reicht aber eine Entnahme der offensichtlich erkennbaren Datenträger (SIM-Karte, Speicherkarte) bei modernen mobilen Kommunikationsmitteln nicht aus. Ebenso ist ein einfaches Zurücksetzen auf den Auslieferungszustand nicht ausreichend. Bei einer Löschung ist insbesondere sicherzustellen, dass alle Adressbucheinträge, verknüpften Zugänge zu Servern (Hersteller, Soziale Netzwerke, Dateiablagen, Clouds), SMS/MMS, Listen der ein- und ausgegangenen Anrufe, im Webbrowser hinterlegte Daten (Passwörter, Cookies, Cache), aber auch durch Anwendungen Dritter gespeicherte Daten und freie Speicherbereiche physisch durch Überschreiben gelöscht werden (vgl. auch Nr. 4.8 im XI. Tätigkeitsbericht: „Vernichtung von Datenträgern – neue DIN 66399“).

Eine weitere Möglichkeit wäre es, eine Datenlöschung in einer Fachwerkstatt oder einem Fachgeschäft vornehmen zu lassen und so z. B. die Herausgabe von teuren Smartphones von der Begleichung der Kosten durch den neuen Eigentümer abhängig zu machen.

Aus datenschutzrechtlicher Sicht wiegen letztlich die schutzwürdigen Interessen des Eigentümers an seinen gespeicherten Daten schwerer als das Recht des Finders, das Gerät nach einer angemessenen Wartezeit als sein Eigentum zu erwerben. Das bedeutet, dass vor einer Weitergabe an Dritte eine komplette Löschung der im Gerät bzw. auf dem Datenträger befindlichen personenbezogenen Daten erfolgen muss. Ist dies nicht möglich, muss die Fundsache datenschutzgerecht entsorgt werden.

4.13 Verschlüsseltes Kontaktformular vs. unverschlüsselte E-Mail

Ein Petent wandte sich an den Landesbeauftragten und beschwerte sich darüber, dass im Rahmen einer Vertragsbeziehung seine vertraulichen Kundendaten unverschlüsselt per E-Mail versendet wurden.

Durch den Vertragspartner wird ein verschlüsseltes Kundenportal zur Verfügung gestellt, welches den Kunden ermöglichen soll, Vertragsdaten online zu verwalten und vertrauliche Anfragen zu übermitteln. Die Aktivitäten im Kundenportal werden durch das mit 128-Bit-AES-Verschlüsselung umgesetzte HTTPS-Protokoll nach Stand der Technik vor Kenntnisnahme durch Unbefugte geschützt.

Der Petent übermittelte über dieses Kundenportal eine vertrauliche Nachricht, in der er seine alte Bankverbindung unter Angabe von Kontonummer und Bankleitzahl widerrief und die aktuelle Bankverbindung unter Angabe von IBAN und BIC mitteilte. Er übermittelte diese sensiblen personenbezogenen Daten in der Annahme, diese seien durch das HTTPS-Protokoll hinreichend geschützt.

Allerdings erhielt der Petent am selben Tag eine unverschlüsselte Bestätigungs-E-Mail, die den gesamten Nachrichtentext aus dem Kundenportal enthielt. Somit wurden die vertraulichen Daten, die verschlüsselt über das Kundenportal übermittelt wurden, unnötigerweise erneut, jedoch diesmal unverschlüsselt zurückgesandt.

Eine Erforderlichkeit für diese Verfahrensweise ist nicht erkennbar, denn eine kurze Bestätigung, dass die Nachricht angekommen ist, wäre aus Sicht des Petenten und auch aus Sicht des Landesbeauftragten ausreichend gewesen. Aus diesem Grund wurde der Vertragspartner aufgefordert, die o. g. Verfahrensweise kurzfristig zu ändern, um zukünftig zu verhindern, dass sensible personenbezogene Kundendaten unverschlüsselt per E-Mail versendet werden und somit die Vertraulichkeit der Daten gefährdet wird. Dieser bedauerte den Vorfall sehr und informierte den Landesbeauftragten über eine geänderte Verfahrensweise, dass nämlich die Kunden ab sofort nur noch eine kurze Bestätigung über das Eintreffen der Nachricht erhalten.

5 Telekommunikation und Medien

5.1 De-Mail und E-Mail made in Germany

Im XI. Tätigkeitsbericht (Nr. 4.5) informierte der Landesbeauftragte über die Entwicklung von De-Mail und die Entstehung der „E-Mail made in Germany“-Initiative.

Ziel der Firmen Telekom, GMX, Web.de, Freenet, 1&1 und Strato ist es, mit „E-Mail made in Germany“ den Sicherheitsstandard bei E-Mails zu erhöhen und mit einem eigenen Qualitäts-Siegel zu versehen. Sichere E-Mail-Adressen werden in den E-Mail-Anwendungen der teilnehmenden Unternehmen besonders gekennzeichnet. E-Mails sollen nur in sicheren, deutschen Rechenzentren gespeichert, immer verschlüsselt transportiert und datenschutzgerecht verarbeitet werden. Eine Ende-zu-Ende-Verschlüsselung ist nicht vorgeschrieben. Die Dienstleistung soll für alle Nutzer kostenlos sein. „E-Mail made in Germany“ ist somit eine sicherere Variante der E-Mail. Im Wesentlichen wird jedoch nur die TLS-Transportverschlüsselung von E-Mails – ein über 15 Jahre alter Internet-Standard (RFC 2487, 3207) – endlich umgesetzt. Datenschutz nach dem „Stand der Technik“ sieht anders aus.

Die technische Absicherung beruht auf dem selbstentwickelten Verfahren „Inter Mail Provider Trust“. Dabei werden sichere Konfigurationen gängiger E-Mail-Server vorgegeben und Angaben der Teilnehmer zu ihrer Infrastruktur nebst Zertifikaten sicher ausgetauscht. Offenbar ist das Interesse, kleinere Anbieter in den Verbund aufzunehmen, wenig ausgeprägt. Mindestens ein E-Mail-Provider kann trotz sicherer Transportwege und Aufnahmeantrag nicht am System teilnehmen und darin als sicher gekennzeichnet werden. Auch ist die Teilnahme am System kostenpflichtig, da die Sicherheit mittels Audits nachgewiesen und zertifiziert werden muss.

Im Unterschied zu De-Mail, bei denen die gegenüber herkömmlichen E-Mails leicht erhöhten Sicherheitsmaßnahmen ähnlich sind, gibt es jedoch keine Identifizierung der beteiligten Absender und Empfänger. Gemeinsam ist beiden die sichere Datenübertragung und die Verarbeitung ihrer Daten in deutschen Rechenzentren.

De-Mail-Sendungen auf der Grundlage des De-Mail-Gesetzes sind zusätzlich rechtssicher und nachweisbar und verfügen über weitere Funktionen, wie z. B. eine Einschreiben-Funktionalität. Die Kritik an De-Mail ist seit dem letzten Tätigkeitsbericht weitgehend unverändert geblieben: praxisferner und nutzloser Virenscan, unnötige Inkompatibilität zum Rest der Welt und verhältnismäßig hohe Kosten. Die immer wieder – zuletzt im Oktober 2013 in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (**Anlage 5**) – geforderte, bisher feh-

lende Ende-zu-Ende-Verschlüsselung wurde im April 2015 durch die „Arbeitsgemeinschaft De-Mail“ nachgerüstet; allerdings nicht im De-Mail-System selbst, sondern als Plugin für die Webbrowser Firefox und Chrome. Dies ist ein erster Schritt hin zur Etablierung einer richtig verschlüsselten, sicheren E-Mail-Kommunikation in der Mitte der Gesellschaft. Jede Behörde wäre nun technisch in der Lage, Ende-zu-Ende-verschlüsselte De-Mails anzunehmen.

Am 1. August 2013 trat das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz – EGovG, BGBl. I S. 2749) in Kraft. Ziel ist es, die elektronische Kommunikation mit der Verwaltung unter anderem durch die Zulassung zweier weiterer sicherer technischer Verfahren zur Ersetzung der Schriftform (eID-Funktion des nPA bei elektronischen Formularen im Internet und absenderbestätigte De-Mails) zu vereinfachen. De-Mails wurden damit zum zulässigen Verfahren zur Behördenkommunikation bestimmt, obwohl keine Komplettverschlüsselung vorgeschrieben wurde. Es liegt nun an den Behörden, De-Mail zu nutzen und den Bürgern auch einen öffentlichen PGP-Schlüssel zur sicheren Kommunikation anzubieten.

Da die De-Mail-Anbieter (Deutsche Telekom, United Internet mit Web.de, GMX, 1&1 und die Mentana-Claimsoft/Francotyp-Postalia Gruppe) teilweise identisch mit den „E-Mail made in Germany“-Anbietern sind, dürfte es nur eine Frage der Zeit sein, bis die PGP-basierte Ende-zu-Ende-Verschlüsselung auch bei den normalen E-Mails allgemein verfügbar und einfach nutzbar sein wird.

Auch andere E-Mail-Provider bieten sichere E-Mail-Transportwege z. B. unter Nutzung offener Standards wie DANE und DNSSEC und damit unabhängig von „E-Mail made in Germany“ und De-Mail an. Vielfach wird kritisiert, dass „E-Mail made in Germany“ der falsche Weg zur Transportwegabsicherung sei und das aufwändiger zu administrierende DANE als offener und unabhängiger Standard, den jeder nutzen kann, bevorzugt werden sollte. DANE beseitigt Schwachstellen der TLS-Transportwegverschlüsselung und erhöht die Sicherheit verschlüsselter Kommunikation, indem die Gegenstellen mittels TLS verschlüsseln und ihre Authentizität überprüfen können. Der Bund setzt für die Webseiten des BSI und seine SMTP-E-Mail-Server DANE ein.

5.2 E-Privacy-Richtlinie

Sowohl in seinem X. als auch in seinem XI. Tätigkeitsbericht (Nr. 25.6 bzw. 4.15) hat der Landesbeauftragte über die Änderung der E-Privacy-Richtlinie 2002/58/EG berichtet. Diese wurde durch die EU-Richtlinie 2009/136/EG u. a. in Art. 5 Abs. 3 dahingehend geändert, dass „die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat.“

Während die E-Privacy-Richtlinie bis dahin eine Widerspruchslösung (Opt-Out) für die Speicherung von Cookies vorsah, dürfen diese nun, wenn sie nicht für die Erbringung des Dienstes erforderlich sind, nur dann verwendet werden, wenn der Nutzer vorher darin einwilligt (Opt-In).

Diese sogenannte „Cookie-Richtlinie“ (EU-Richtlinie 2009/136/EG) hätte bis 25. Mai 2011 in nationales Recht umgesetzt und anstelle der bisherigen Widerspruchsregelung in § 15 Abs. 3 Telemediengesetz (TMG) eine Einwilligungsregelung geschaffen werden müssen. Allerdings wurde ein auf Initiative der SPD-Bundestagsfraktion eingebrachter Gesetzentwurf vom 24. Januar 2012 (BT-Drs. 17/8454) zur Schaffung eines neuen § 13 Abs. 8 TMG abgelehnt. Die Bundesregierung hält die derzeit geltenden Vorgaben des TMG für ausreichend und sieht keinen weiteren Umsetzungsbedarf.

Aus diesem Grund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Februar 2015 eine Entschließung verabschiedet, in der sie die Bundesregierung auffordert, den Bürgerinnen und Bürgern ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung der Privatsphäre bei der Nutzung des Internets nicht weiter vorzuenthalten und die E-Privacy-Richtlinie nun ohne weitere Verzögerung vollständig in nationales Recht zu überführen (**Anlage 21**).

5.3 Webtracking und Privatsphäre

Device Fingerprinting ist eine Form des Webtracking, die ohne das Setzen von Cookies auskommt. Dabei werden auf Computern, Smartphones, Tablets oder anderen Endgeräten (engl. Devices) Informationen über die Systemkonfiguration, wie z. B. den verwendeten Browser, das genutzte Betriebssystem, installierte Schriftarten, die Bildschirmauflösung, installierte Plugins, MAC- oder IP-Adressen, ausgelesen. Eine Identifizierung des Nutzers erfolgt über die Auswertung dieser Systeminformationen, die wie ein individueller Fingerabdruck wirken. Im Gegensatz zum Webtracking durch Cookies, welches durch ein Sperren oder Löschen der Cookies relativ einfach unterbunden werden kann, ist Webtracking durch Device Fingerprinting für den Nutzer nicht ohne Weiteres zu erkennen und erst recht nicht zu unterbinden. Die Übermittlung dieser Systeminformationen erfolgt oft automatisch an den jeweiligen Webserver, ohne aktives Handeln der Nutzer, z. B. durch den Webbrowser selbst.

Aus diesem Grund hat die Artikel-29-Datenschutzgruppe, der Zusammenschluss nationaler Datenschutzaufsichtsbehörden auf EU-Ebene, im November 2014 eine Stellungnahme veröffentlicht (Opinion 09/2014 on the application of Directive 2009/136/EG to Device Fingerprinting), die sich mit der Frage beschäftigt, ob die als „Cookie-Richtlinie“ bekannt gewordene Richtlinie 2009/136/EG auch auf Device Fingerprinting Anwendung findet und somit auch hier ein Einwilligungserfordernis besteht (siehe Nr. 5.2).

Im Ergebnis kommt die Artikel-29-Datenschutzgruppe zu der Einschätzung, dass Device Fingerprinting den Anforderungen der E-Privacy- bzw. Cookie-Richtlinie unterliegt und diese Technologie somit nur mit Einwilligung des Nutzers eingesetzt werden darf. Allerdings sieht die E-Privacy-Richtlinie grundsätzlich zwei Ausnahmen von der Einwilligungspflicht vor: Entweder „wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist“ oder „wenn der Zugriff unbedingt erforderlich ist, um den vom Teilnehmer oder Nutzer gewünschten Dienst zur Verfügung zu stellen“. Eingesetzt wird Device Fingerprinting aber vor allem zur verhaltensorientierten Werbung sowie zu Analyse- und Sicherheitszwecken.

Der Landesbeauftragte empfiehlt allen Anbietern von Telemedien, sowohl bei der Verwendung herkömmlicher Cookies als auch beim Einsatz von Device Fingerprinting, eine Einwilligung des Nutzers einzuholen, um die Auswertung des Nutzerverhaltens datenschutzkonform zu gestalten.

5.4 EU-Verordnung über elektronische Identifizierung und Vertrauensdienste

Der Landesbeauftragte hat in seinem XI. Tätigkeitsbericht (Nr. 4.3) über den Entwurf einer Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und die damit verbundenen datenschutzrechtlichen Probleme berichtet. Im April 2014 hat das Europaparlament in Abstimmung mit dem Europäischen Rat dem Vorschlag für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS VO) zugestimmt. Damit sind alle Mitgliedstaaten verpflichtet, die Systeme zur elektronischen Identifizierung anderer EU-Länder offiziell anzuerkennen. Die Verordnung gilt seit September 2014 und muss in Teilen ab dem 1. Januar 2016 umgesetzt werden.

Für die Bürgerinnen und Bürger sowie für Unternehmen in Deutschland bedeutet die eIDAS VO, dass sie sich z. B. mit dem Personalausweis bei Behörden europaweit elektronisch identifizieren können. Entsprechend müssen deutsche Behörden künftig den elektronischen Ausweis anderer EU-Länder anerkennen. Die eIDAS VO bezieht sich außerdem auf elektronische Signaturen, Zeitstempel und Siegel sowie Verfahren zur Webseiten-Authentifizierung.

Mit Wirkung vom 1. Juli 2016 wird die bislang gültige Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie) aufgehoben. Da die eIDAS VO – anders als die bisherige Richtlinie – wie ein deutsches Bundesgesetz direkt gilt, ersetzt sie auch das deutsche Signaturgesetz von 2001.

Welche Folgen die Verordnung für die qualifizierte elektronische Signatur in Deutschland haben wird, wenn europaweit nur fortgeschrittene Signaturen – mit einem geringeren Sicherheitsniveau – gelten, muss sich noch zeigen. Auf jeden Fall werden zukünftig auch solche Signaturen aus europäischen Mitgliedstaaten in Deutschland anerkannt werden müssen.

5.5 Sind IP-Adressen personenbezogene Daten?

Seit vielen Jahren wird die Frage, ob IP-Adressen personenbezogene Daten sind und damit dem Datenschutzrecht unterfallen, kontrovers diskutiert. Eine Grundsatzentscheidung des Europäischen Gerichtshofs (EuGH) könnte darauf eine Antwort liefern.

Der Bundesgerichtshof (BGH) hat in einem Rechtsstreit zu klären, ob die Bundesregierung die IP-Adressen ihrer Webseiten-Besucher auch über den jeweiligen Nutzungsvorgang hinaus speichern darf. Begründet wird dies mit dem Ziel, Angriffe abwehren und Angreifer so besser strafrechtlich verfolgen zu können. Neben der IP-Adresse werden auch der Name der abgerufenen Seite und der Zeitpunkt des Abrufs gespeichert.

Der Kläger sieht darin einen Verstoß gegen das Telemediengesetz (TMG) und hatte die Bundesregierung auf Unterlassung verklagt. Während das Amtsgericht Tiergarten die Klage im August 2008 abgewiesen hat (Az. 2 C 6/08), räumte das Landgericht Berlin dem Kläger einen Unterlassungsanspruch für den Fall ein, dass auf der Webseite zugleich persönliche Daten erhoben werden. An sich seien IP-Adressen aber keine personenbezogenen Daten (Az. 57 S 87/08). Gegen das Urteil legten beide Parteien Revision ein.

Allerdings hat der BGH das Revisionsverfahren im Oktober 2014 ausgesetzt und dem EuGH Fragen zur Auslegung der Datenschutz-Richtlinie 95/46/EG vorgelegt (Beschluss vom 28. Oktober 2014, Az. VI 135/13). So soll geklärt werden, ob IP-Adressen personenbezogene Daten sind und ob das europäische Datenschutzrecht in der Frage der Nutzung personenbezogener Daten eventuell mehr Spielraum lässt als das deutsche TMG. Ein Diensteanbieter darf personenbezogene Daten eines Nutzers gemäß § 15 Abs. 1 TMG nämlich nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen bzw. gemäß § 12 Abs. 1 TMG, wenn der Nutzer eingewilligt hat. Artikel 7 Buchstabe f der Datenschutz-Richtlinie lässt dagegen die Verarbeitung personenbezogener Daten zur Verwirklichung eines berechtigten Interesses zu, sofern nicht das Interesse der Betroffenen oder deren Grundrechte überwiegen.

Die Datenschutzbeauftragten vertreten schon seit jeher die Auffassung, dass die IP-Adresse ein personenbezogenes Datum darstellt. Dies wird u. a. in einem Beschluss des Düsseldorfer Kreises vom 26. bis 27. November 2009 zur „Datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ deutlich (vgl. X. Tätigkeitsbericht, Nr. 14.6, Anlage 24). Die Entscheidung des EuGH wird sowohl für die einheitliche Auslegung geltenden Rechts als auch für die zukünftige Datenschutzgrundverordnung von entscheidender Bedeutung sein.

5.6 Vom Fernseher zum Smart-TV

Datenschutzrechtliche Forderungen

Moderne Fernsehgeräte bieten neben dem klassischen, passiven Fernsehempfang auch eine Vielzahl an Möglichkeiten, aktiv das Internet zu nutzen. Die Zuschauer können zeitgleich im Internet recherchieren, Einkäufe tätigen oder E-Mail-Dienste nutzen und über HbbTV Zusatzinformationen zur gerade laufenden Fernsehsendung oder Inhalte von Mediatheken abrufen (Smart-TV).

Durch die Verbindung zum Internet entsteht – anders als beim bisherigen Fernsehen – ein sogenannter Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Viele Geräte sind ab Werk so voreingestellt, dass bereits beim ersten Anschalten und beim normalen Fernsehempfang Daten weitergeleitet werden. Auf diese Weise lässt sich nicht nur das Fernseh- und Internetverhalten der Zuschauer ausforschen, sondern es können zukünftig auch umfangreiche Profile über Tagesabläufe, Nutzungsgewohnheiten und persönliche Interessen entstehen.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang

ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erhebung und Auswertung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus diesem Grund haben die Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis) und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten im Mai 2014 ein gemeinsames Positionspapier veröffentlicht, welches auch von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt wird (**Anlage 39**).

Die wichtigste Forderung des Positionspapiers ist die Gewährleistung der anonymen Nutzung von Fernsehangeboten auch bei der Verwendung von Smart-TV. Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Grundsatz der anonymen Nutzung hinreichend Rechnung getragen wird („privacy by default“). Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

Technische Prüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat Smart-TV-Geräte von dreizehn Herstellern, die etwa 90% des Marktes in Deutschland abdecken sollen, daraufhin untersucht, welche Daten bei Nutzung der Geräte fließen und ob eine Datenschutzerklärung vorhanden ist. Neben Bayern haben die Hersteller der Smart-TV-Geräte ihren Sitz in Berlin, Hamburg, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz. Die Datenschutzaufsichtsbehörden dieser Länder haben das BayLDA im Wege der Amtshilfe mit der technischen Prüfung dieser Geräte beauftragt. Im Dezember 2014 und im Januar 2015 wurden die Prüfungen im Beisein von Vertretern der Gerätehersteller durchgeführt und Mitte Februar 2015 den Aufsichtsbehörden die Prüfberichte übersandt. Die Ergebnisse der Prüfung wurden im Rahmen einer Pressekonferenz am 27. Februar 2015 geräteübergreifend präsentiert und auch auf der Homepage des BayLDA veröffentlicht.

Es wurden verschlüsselte Datenflüsse vom Gerät zum Hersteller festgestellt bei der Nutzung des elektronischen Programmführers, bei der Wiedergabe externer Inhalte von USB-Sticks, bei der Aufnahme von Fernsehsendungen und auch beim „normalen“ Fernsehen. Die Einwilligung in die Nutzung sämtlicher Daten war dabei Voraussetzung. Die Gerätehersteller waren allerdings nicht bereit, die Zertifikate zur Entschlüsselung der Datenflüsse für die Prüfung bereitzustellen.

Um Datenflüsse vom Gerät zu HbbTV-Anbietern zu analysieren, wurden zehn Fernsehsender (fünf öffentlich-rechtliche, fünf private) ausgewählt. Dabei wurde u. a. festgestellt, dass bei sieben von zehn Sendern ein Tracking beim Senderwechsel erfolgt, sodass die Verweildauer bei einem bestimmten Sender und der Wechsel zu einem anderen Sender nachverfolgt werden können. Beim „normalen“ Fernsehen sind bei allen zehn Fernsehsendern Datenflüsse vom Gerät zum Sender festzustellen, wobei hier wiederum in sämtliche Datennutzung eingewilligt wurde. Eine Datenschutzerklärung war bei acht Sendern vorhanden.

5.7 Rundfunkfinanzierung – Sachstand

Bereits in seinem X. und XI. Tätigkeitsbericht (Nr. 25.2 bzw. 4.12) berichtete der Landesbeauftragte über den 15. Rundfunkänderungsstaatsvertrag und die damit verbundene Einführung des neuen Rundfunkbeitrags.

Im Zuge der Ratifikation des Staatsvertrages hatten sich die Länder darauf verständigt, den Rundfunkbeitrag zeitnah zu evaluieren. Hierzu wurde Anfang 2012 eine Arbeitsgruppe unter Federführung des Landes Baden-Württemberg eingesetzt und die DIW Econ, ein Consulting-Tochterunternehmen des Deutschen Instituts für Wirtschaftsforschung in Berlin, mit der unabhängigen, externen Begleitung des Evaluationsprozesses beauftragt.

Mit den Ergebnissen dieser Evaluierung haben sich die Regierungschefinnen und Regierungschefs der Länder am 18. Juni 2015 befasst und Eckpunkte beschlossen, auf deren Grundlage eine Änderung des Rundfunkbeitragsstaatsvertrages vorbereitet wird. Die Eckpunkte basieren auf dem Bericht der Rundfunkkommission zur Evaluierung des Rundfunkbeitrags einschließlich der dem Bericht zugrunde liegenden Evaluierungsberichte des DIW Econ und der Rundfunkanstalten.

Aus datenschutzrechtlicher Sicht zu begrüßen ist der Verzicht auf die Vorlage von Originalen oder amtlichen Beglaubigungen zum Nachweis der Befreiungs- bzw. Ermäßigungsvoraussetzungen. Ausreichend ist nun eine einfache Kopie der behördlichen Bestätigung. Dadurch wird verhindert, dass beim Einscannen des gesamten Leistungsbescheides nicht erforderliche personenbezogene Daten der Antragsteller erhoben und verarbeitet werden.

Des Weiteren sollen bestimmte Vorgaben für die Datenerhebung, die bisher nur in den Satzungen der Rundfunkanstalten enthalten waren, in den Rundfunkbeitragsstaatsvertrag übernommen werden. Das gilt insbesondere für die Regelung, dass eine Datenerhebung bei Dritten voraussetzt, dass die Datenerhebung beim Betroffenen erfolglos war oder nicht möglich ist.

Allerdings ist auch geplant, einen weiteren vollständigen Meldedatenabgleich durchzuführen, um zur dauerhaften Sicherung der Beitragsgerechtigkeit und Stabilisierung der Beitragseinnahmen beizutragen. Im Gegenzug könnte auf die Befugnis zum Adressankauf und zur Vermieterauskunft verzichtet werden.

Da die Meldegesetze der Länder bereits vorsehen, im Falle der Anmeldung einer alleinigen oder Hauptwohnung, einer An- oder Abmeldung einer Nebenwohnung oder des Todes die Meldedaten volljähriger Einwohner an die Rundfunkanstalten zu übermitteln, ist aus datenschutzrechtlicher Sicht die Forderung nach einem nochmaligen vollständigen Meldedatenabgleich nicht nachvollziehbar. Hier sind die Rundfunkanstalten aufgefordert, konkrete Fallzahlen vorzulegen, die die Erforderlichkeit einer solchen Maßnahme rechtfertigen.

Trotz der Einwände der Datenschutzbeauftragten wurde der Staatsvertrag zur Änderung des Rundfunkbeitragsstaatsvertrages (19. Rundfunkänderungsstaatsvertrag) im

Rahmen der Ministerpräsidentenkonferenz am 3. Dezember 2015 von den Regierungschefinnen und Regierungschefs unterzeichnet.

5.8 Soziale Netzwerke

5.8.1 Nutzung sozialer Netzwerke durch öffentliche Stellen

Auch im vergangenen Berichtszeitraum gab es Anfragen öffentlicher Stellen zur Nutzung sozialer Netzwerke, insbesondere von Facebook-Fanpages. An der Empfehlung des Landesbeauftragten aus seinem XI. Tätigkeitsbericht (Nr. 4.19.1), auf die Einrichtung solcher Seiten zu verzichten, hat sich jedoch nichts geändert. Der Grund dafür sind die nach wie vor bestehenden datenschutzrechtlichen Probleme und die diesbezüglich ausstehenden abschließenden Gerichtsentscheidungen.

Auch die länderoffene Arbeitsgruppe des Arbeitskreises I der Innenministerkonferenz, die ihren Bericht zum Datenschutz in sozialen Netzwerken vom 4. April 2012 fortgeschrieben hat, stellt in dem Bericht zur Fortentwicklung des Sachstandes vom 31. Juli 2013 fest, dass es keinen Anlass gibt, die Handlungsempfehlungen vom April 2012 grundlegend zu korrigieren.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte Ende 2011 kritisiert, dass die Datenverarbeitung bei Facebook nicht mit deutschem Datenschutzrecht vereinbar ist, u. a. weil die Nutzung von Fanpages personenbezogen präzise erfasst wird, gegen die Profilbildung keine Widerspruchsmöglichkeit eingeräumt wird, beim Setzen von Cookies keine wirksamen Einwilligungen eingeholt werden und weil für die Betroffenen nicht die geforderte Transparenz hergestellt wird. Daraufhin wurden drei Unternehmen in Schleswig-Holstein per Verfügung aufgefordert, ihre Fanpages zu deaktivieren. Diese reichten Klage ein.

Daraufhin stellte das Schleswig-Holsteinische Verwaltungsgericht in seinem Urteil vom 9. Oktober 2013 fest, dass deutsche Betreiber von Facebook-Fanpages für die bei Facebook erfolgende Datenverarbeitung datenschutzrechtlich in keiner Weise verantwortlich gemacht werden können (Az. 8 A 37/12, 8 A 14/12, 8 A 218/11). Wegen der grundsätzlichen Bedeutung der Urteile ließ das Gericht jedoch die Berufung zu, welche vom ULD am 1. November 2013 eingelegt wurde.

Mit Urteil vom 4. September 2014 wurde die Berufung zurückgewiesen. Der 4. Senat des Schleswig-Holsteinischen Oberverwaltungsgerichtes (Az. 4 LB 20/13) entschied, dass der Betreiber einer Facebook-Fanpage für die allein von Facebook vorgenommene Verarbeitung personenbezogener Daten von Besuchern der Fanpage datenschutzrechtlich nicht verantwortlich ist, da er keinen Einfluss auf die technische und rechtliche Ausgestaltung der Datenverarbeitung durch Facebook hat. Dass er von Facebook anonyme Statistikdaten über Nutzer erhält, begründet keine datenschutzrechtliche Mitverantwortung. Da das Oberverwaltungsgericht die Revision zugelassen hatte, weil entscheidende Rechtsfragen bisher nicht höchstrichterlich entschieden wurden, hatte das ULD im Januar 2015 das Urteil vor dem Bundesverwaltungsgericht angefochten. Die Entscheidung und deren Begründung bleiben abzuwarten.

Unabhängig von künftigen Gerichtsentscheidungen ist festzustellen, dass es zwar zutrifft, dass Betreiber einer Facebook-Fanpage keinen Einfluss auf die technische

und rechtliche Ausgestaltung der Verarbeitung personenbezogener Daten bei Facebook haben. Die datenschutzrechtliche Verantwortung besteht aber aus Sicht des Landesbeauftragten insbesondere dann, wenn eine öffentliche Stelle, die gem. Art. 20 Abs. 3 GG an Recht und Gesetz gebunden ist, Anbieter von Internetdiensten auswählt, die die deutschen Datenschutzvorschriften nicht einhalten.

Einer der weiteren datenschutzrechtlichen Kritikpunkte betrifft die Klarnamenpflicht für Facebook-Nutzer. Diese ist Gegenstand einer Anordnung, die der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit am 24. Juli 2015 gegen die Facebook Irland Ltd. erlassen hat. Neben dem Verstoß gegen § 13 Abs. 6 Telemediengesetz (Recht auf pseudonyme Nutzung) geht es in der Anordnung auch um den Verstoß gegen die Speicherverbote aus § 20 Abs. 2 Personalausweisgesetz und § 18 Abs. 3 Passgesetz.

Facebook wird darin verpflichtet, die pseudonyme Nutzung seines Dienstes zuzulassen. Die Sperrung eines Nutzerkontos, die aufgrund der pseudonymen Nutzung vorgenommen wurde, ist aufzuheben. Weiter wird angeordnet, dass Facebook die einseitige Änderung des Kontos auf den wirklichen Namen des Nutzers zu unterlassen hat. Außerdem ist die Forderung der Vorlage von amtlichen Lichtbildausweisen (Personalausweis oder Reisepass) zum Identitätsnachweis durch Übersendung digitaler Kopien unzulässig.

Hintergrund der Verwaltungsanordnung ist die Beschwerde einer Nutzerin, die ihr Konto bei Facebook unter einem Pseudonym geführt hatte. Dadurch wollte sie erreichen, dass ihr privates Konto auf Facebook nicht zur geschäftlichen Kontaktaufnahme durch Dritte genutzt wird. Facebook hatte daraufhin das Konto gesperrt und die Betroffene aufgefordert, ihren echten Namen im Profil anzugeben. Außerdem sollte sie ihre Identität durch einen amtlichen Lichtbildausweis beweisen; ein von ihr eingereichter anderer Identitätsnachweis reichte Facebook nicht aus. Gegen ihren Willen änderte Facebook zudem den Profilnamen vom Pseudonym in den wirklichen Namen der Betroffenen. Dadurch gab Facebook den echten Namen der Nutzerin ihren „Freunden“ bekannt. Die Freischaltung des Kontos für die Nutzerin soll allerdings erst dann erfolgen, wenn die Nutzerin dieser Änderung zustimmt. Sie hat es jedoch vorgezogen, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

Facebook hat gegen die Anordnung bereits Widerspruch eingelegt und beim Verwaltungsgericht Klage erhoben.

5.8.2 Datenschutzkonforme Nutzung von Social Plugins

Auf einer Vielzahl von Webseiten findet man den „Gefällt-mir“-Button von Facebook, den „g+1“-Button von Google+ oder den „Tweet“-Button von Twitter. Mit diesen Social Plugins können Inhalte durch Nutzer auf Facebook, Google oder Twitter gepostet und hierdurch eine Vielzahl weiterer Nutzer erreicht werden. Der von den sozialen Netzwerken bereitgestellte Quellcode wird in der Regel als iFrame in die eigenen Webseiten eingebunden. Das führt dazu, dass beim Aufruf der Seiten immer Nutzerdaten auch dann an Facebook, Google und Twitter übermittelt werden, wenn der Webseitenbesucher die Buttons gar nicht anklickt.

Aus diesem Grund sollten die von den sozialen Netzwerken bereitgestellten Social Plugins nicht direkt in die Webseite eingebunden werden, sondern z. B. mittels einer

sogenannten 2-Klick-Lösung. Dabei werden zunächst deaktivierte Buttons verwendet, die keinen Kontakt mit den Servern der sozialen Netzwerke herstellen. Erst wenn der Nutzer diese aktiviert und damit seine Zustimmung erklärt, werden die Buttons aktiv und stellen die Verbindung her.

Eine weitere Möglichkeit ist die Einbindung eigener, individuell gestalteter Buttons, bei denen die Kommunikation mit den sozialen Netzwerken ein auf dem eigenen Server abgelegtes Skript übernimmt, welches erst Daten überträgt, wenn der Nutzer einen Button betätigt.

5.8.3 Facebook ändert Nutzungsbedingungen

Zum 30. Januar 2015 hat Facebook seine Nutzungsbedingungen und Datenverwendungsrichtlinie geändert. Wie auch schon bei vorangegangenen Änderungen hatten die Nutzer jedoch keine Möglichkeit zu widersprechen. Wer nicht einverstanden war, durfte sich ab dem 30. Januar nicht mehr im Netzwerk anmelden, da er ansonsten den Änderungen automatisch zugestimmt hätte.

Die wichtigste Änderung betrifft die Erstellung von Werbeprofilen der Nutzer. Bislang wurden diese Werbeprofile vor allem auf Grundlage des Verhaltens der Nutzer im sozialen Netzwerk erstellt. Wer etwas teilt oder mit einem "Gefällt mir" versieht, übermittelt Facebook seine Interessen und Vorlieben. Durch die Verwendung von Cookies und Social Plugins ist Facebook jedoch ebenso in der Lage, die Aktivitäten seiner eingeloggten Nutzer im Netz nachzuvollziehen. Deshalb sollen in Zukunft auch besuchte Internetseiten und genutzte Apps ausgewertet werden.

Um den Nutzern die Entscheidung zu erleichtern, wer ihre Inhalte sehen darf, stellt Facebook interaktive Anleitungen zur Verfügung und bietet auch Möglichkeiten, die Analyse von besuchten Seiten und Apps zu kontrollieren. Allerdings muss der Nutzer hier aktiv werden. Neue Funktionen müssen in der Regel deaktiviert werden, wenn man mit ihnen nicht einverstanden ist (Widerspruchsprinzip). Der Nutzer muss sich jedoch bewusst sein, dass trotz aller Einstellungen Facebook selbst immer alles erfährt und möglicherweise auswertet.

Da die Facebook Germany GmbH ihren Sitz in Hamburg hat, ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) die zuständige Datenschutzaufsichtsbehörde. Dieser teilte mit, dass eine kritische Durchsicht der angekündigten Änderungen datenschutzrechtliche Zweifel an der Zulässigkeit des beschriebenen Umfangs und der Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Nutzer aufkommen lassen. Er werde insbesondere klären, ob der in der Neuformulierung der Datenrichtlinie beschriebene Austausch personenbezogener Daten mit den als „Facebook-Unternehmen“ bezeichneten Drittunternehmen (z. B. WhatsApp, Instagram, Atlas), vor allem unter Einbeziehung der von diesen Unternehmen verwendeten Datenschutzerklärungen, zulässig sei. Der in der Datenrichtlinie beschriebene Umfang und die Art der Datenverarbeitung müssten außerdem im Einklang mit den Prinzipien der Zweckbindung und Transparenz der Datenverarbeitung sowie der Datensparsamkeit und Datenvermeidung stehen.

In diesem Zusammenhang hat der HmbBfDI Facebook um die Beantwortung einiger Fragen gebeten und ein Prüfverfahren angekündigt. Diese Fragen wurden von Facebook nicht beantwortet. Vielmehr vertritt Facebook Irland die Auffassung, dass Fa-

cebook nur dem irischen Datenschutzrecht unterworfen sei. Weder das BDSG noch das TMG seien auf die Aktivitäten von Facebook anwendbar. Entsprechend hätte der HmbBfDI gegenüber Facebook auch keinerlei aufsichtsbehördliche Zuständigkeit oder Befugnisse. Mit dieser Argumentation entzieht sich Facebook einer inhaltlichen und datenschutzrechtlichen Auseinandersetzung mit seiner neuen Datenrichtlinie auf nationaler Ebene.

Die Rechtsauffassung von Facebook wird durch den HmbBfDI nicht geteilt. Facebook ist der Pflicht zur Auskunftserteilung gemäß BDSG nicht nachgekommen, deshalb werden nun die erforderlichen rechtlichen Maßnahmen ergriffen, um den Auskunftsanspruch gegenüber der verantwortlichen Stelle durchzusetzen.

5.9 Biometrische Gesichtserkennung durch Internetdienste

Bereits im Dezember 2010 hatte Facebook seine Gesichtserkennungsfunktion eingeführt. Diese war für alle Mitglieder automatisch aktiviert und konnte nur nachträglich ausgeschaltet werden (Opt out). Standardmäßig wurden alle eingestellten Fotos analysiert. Die Nutzer hatten die Möglichkeit, Freunde in hochgeladenen Bildern zu markieren und so die Fotos mit Namen zu versehen. Eine Einwilligung erfragte Facebook von seinen Nutzern dafür nicht.

Der HmbBfDI hatte im September 2012 gegenüber der Facebook Inc. eine Verwaltungsanordnung erlassen. Darin wurde das US-Unternehmen dazu verpflichtet, das Verfahren der Gesichtserkennung auch rückwirkend datenschutzkonform zu gestalten. Facebook sollte sicherstellen, dass nur mit einer aktiven Zustimmung der bereits registrierten Nutzer biometrische Profile erzeugt und dauerhaft gespeichert werden. Außerdem sollten die Nutzer vorher umfassend über die Risiken des Verfahrens informiert werden.

Dem Erlass der Anordnung waren langwierige Verhandlungen mit dem Unternehmen vorausgegangen, die letztlich aber scheiterten. Auf dem Verhandlungsweg war Facebook nicht dazu zu bewegen, das Verfahren an europäische Datenschutzstandards anzupassen. Auch in dem der Anordnung vorgeschalteten Anhörungsverfahren hatte Facebook keine neuen Argumente oder Lösungsvorschläge geliefert.

Im Februar 2013 wurde die Anordnung durch den HmbBfDI aufgehoben, da Facebook sich Mitte Oktober 2012 dazu entschlossen hatte, die Gesichtserkennung für alle europäischen Mitglieder zu deaktivieren und im Nachgang einen Nachweis über die Löschung der bis dahin erfassten biometrischen Daten lieferte. Hierzu hatte Facebook überprüfbare Auszüge aus dem benutzten Programmcode vorgelegt. Die dabei gewonnenen Erkenntnisse wurden zudem vom irischen Datenschutzbeauftragten, der eigene Untersuchungen angestellt hatte, bestätigt.

Außerhalb Europas bietet Facebook die Gesichtserkennungsfunktion weiterhin an und arbeitet an der Weiterentwicklung dieses Verfahrens mittels der Software Deep Face. Mit dieser soll sich die Erkennungsrate zukünftig noch wesentlich verbessern. Da aber nicht nur Facebook, sondern auch immer mehr andere Unternehmen die Möglichkeit der Gesichtserkennung für ihre Geschäftszwecke nutzen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Sitzung am 27. und 28. März 2014 eine Entschließung zur biometrischen Gesichtserkennung durch Internetdienste verabschiedet (**Anlage 10**). Darin wird gefordert, dass die Ver-

arbeitung biometrischer Gesichtsmerkmale der Nutzer in sozialen Medien nur mit deren ausdrücklicher und informierter Einwilligung erfolgen darf. Da die biometrischen Daten der Nutzer bei diesen Verfahren dauerhaft und reproduzierbar gespeichert werden, ist das Missbrauchspotential derartiger Gesichtsdatenbanken immens. Das informationelle Selbstbestimmungsrecht der Betroffenen muss daher bei der Erhebung und Verarbeitung von biometrischen Daten in jedem Fall gewahrt werden.

5.10 Einsatz von WhatsApp und anderen Instant Messenger

Vielfach besteht im Land der Wunsch, moderne Kommunikationsmittel zur besseren Vernetzung aller Beteiligten zu verwenden. Sei es z. B. bei der Polizei oder in Schulen, überall gibt es den Trend, die vielfach frei erhältlichen bzw. frei zugänglichen Anwendungen, Apps oder Websites zur Kommunikation und zum Aufbau sozialer Netzwerke zu nutzen.

WhatsApp ist eine Plattform zum Austausch von Nachrichten aller Art (Text, Bild, Video). Das amerikanische Unternehmen ist bereits von je her aufgrund mangelnden Datenschutzes in der Kritik. Zum Einen, weil es die Adressbücher der Nutzer automatisiert und heimlich durch ungeschützte Übertragung (Stiftung Warentest 02/2014: Datenschutz "sehr kritisch") in die eigenen Datenbestände integriert und so selbst zu noch gar nicht existenten Nutzern Profile bildet und deren Daten unerlaubt nutzt. Zum anderen, weil auf Sicherheitslücken nicht, zu spät oder unpassend reagiert wurde. So war das Passwort eines Zugangs mit einfachen Zusatzinformationen errechenbar, Sicherheitslücken erlaubten das Auslesen von Zahlungsdaten von PayPal und Google Wallet, es ließen sich Nachrichten im fremden Kontext versenden. Lange Zeit erfolgte das Versenden von Nachrichten unverschlüsselt und auch derzeit nur mit einer unzureichenden Verschlüsselung. Auch ist es für Dritte leicht möglich, Aktivitätsprofile einzelner Nutzer anhand ihrer Handynummer zu erstellen, ohne dass dies dem Nutzer bekannt wird. Das Unternehmen wurde mittlerweile durch Facebook aufgekauft, die Daten befinden sich demnach wohl auch auf amerikanischen Servern.

Nutzer der Anwendung WhatsApp übertragen über die akzeptierten AGB alle Rechte an der Kommunikation an das Unternehmen WhatsApp.com. Dieses kann anschließend alle Inhalte, Bilder, geografische Positionen, Statusmeldungen usw. ohne Einschränkung und in allen Medienformaten und über alle Kanäle weiterverbreiten. Auch ist das Verkaufsziel der Anwendung viral, d. h. nach einem Jahr kostenloser Nutzung und Werbung unter den eigenen Kontakten, werden die Nutzer zum Abonnement verpflichtet oder WhatsApp sperrt den Zugang komplett, sodass durch den Druck der eigenen Kontakte zahlende Nutzer generiert werden. Angesichts des hohen Kaufpreises von WhatsApp (19 Mrd. $) ist mit hoher Wahrscheinlichkeit anzunehmen, dass Facebook die personenbezogenen Daten der WhatsApp-Nutzer vermarkten wird.

Zwischenzeitlich soll WhatsApp eine sichere Ende-zu-Ende-Verschlüsselung implementiert haben. Diese soll derzeit jedoch nur für Android und nicht z. B. für iOS zur Verfügung stehen. Des Weiteren soll die sichere Verschlüsselung nicht für Gruppen-Chats oder Nachrichten mit Medieninhalten eingesetzt werden können. Die weitere Entwicklung bleibt daher noch abzuwarten. WhatsApp könnte damit unter Umständen (richtige Implementierung, keine Schlüsselhinterlegung, keine bewusst einge-

bauten Schwachstellen, Unterstützung auch anderer Plattformen, …) in der Zukunft datenschutzgerecht genutzt werden.

Eine datenschutzkonforme Nutzung von WhatsApp ist derzeit nicht möglich. Eine gesetzliche Grundlage, welche zur Nutzung verpflichtet, gibt es nicht. Es ist dringend davon abzuraten, WhatsApp für personenbezogene Daten Dritter zu nutzen. Auch sonst kann eine Freiwilligkeit der Nutzung nicht angenommen werden. Die Nutzung sollte daher eingestellt bzw. auf Notfälle begrenzt werden. Die Teilnehmer am Chat sind in einer geschlossenen Benutzergruppe zu verwalten, sodass keine dritten Personen aus dem Internet Zugriff auf personenbezogene Daten erhalten können. Inwieweit unbefugte Dritte seitens des Herstellers bzw. der Server-Administration oder der NSA Zugriffsrechte haben, ist nicht bekannt. Die Sicherheitsvorfälle in der Vergangenheit sollten jedoch nicht unberücksichtigt bleiben. Ob die technischen Anforderungen des DSG LSA/BDSG für den Umgang mit personenbezogenen Daten erfüllt werden, ist mittelfristig anzunehmen, jedoch gibt es keine belastbaren Fakten seitens des WhatsApp-Herstellers.

Eine konkrete Empfehlung für eine aus Datenschutz-Sicht geeignetere Software kann derzeit nicht gegeben werden, da serverbasierte Anwendungen erst installiert und sicher konfiguriert werden müssten und eben dies derzeit nicht zentral angeboten und damit einfach nutzbar ist.

5.11 Google – Datenschutzbestimmungen

Bereits in seinem XI. Tätigkeitsbericht (Nr. 4.20) berichtete der Landesbeauftragte über die seit 1. März 2012 geltenden neuen Datenschutzbestimmungen bei Google, die dazu führten, dass alle Accounts der verschiedenen Google-Dienste zu einem zentralen Google-Account und die zu den einzelnen Diensten gespeicherten Nutzerprofile zu einem einzigen Profil zusammengefasst wurden.

Die neuen Datenschutzbestimmungen wurden trotz erheblicher Bedenken der in der Artikel-29-Datenschutzgruppe auf EU-Ebene zusammengeschlossenen nationalen Datenschutzaufsichtsbehörden durch Google in Kraft gesetzt. Die Behörden hatten sich daher auf ein abgestimmtes Verfahren im Rahmen einer Taskforce geeinigt, bei dem die jeweiligen nationalen aufsichtsbehördlichen Möglichkeiten zum Einsatz kommen sollten. Neben der federführenden Aufsichtsbehörde von Frankreich, den Aufsichtsbehörden von Italien, den Niederlanden, Spanien sowie dem Vereinigten Königreich nahm auch der HmbBfDI an der für das gemeinsame Vorgehen gegründeten Taskforce teil, da die deutsche Niederlassung von Google ihren Sitz in Hamburg hat.

Im Juli 2013 leitete der HmbBfDI ein Verwaltungsverfahren gegen die Google Inc. ein. Zwar konnten in zahlreichen Gesprächen mit Google Verbesserungen insbesondere bei der Information der Nutzer erreicht werden. Bei der wesentlichen Frage der Zusammenführung der Nutzerdaten war Google jedoch nicht bereit, die rechtlich erforderlichen Maßnahmen einzuhalten. Aus diesem Grund erließ der HmbBfDI im September 2014 gegenüber Google eine Verwaltungsanordnung zur Beseitigung von Verstößen gegen das Telemediengesetz und das Bundesdatenschutzgesetz. Google wird darin verpflichtet, Daten, die bei der Nutzung unterschiedlicher Google-Dienste anfallen, nur unter Beachtung der gesetzlichen Vorgaben zu erheben und zusammenzuführen. Die bisherige Praxis der Erstellung von Nutzerprofilen greift weit über

das zulässige Maß hinaus in die Privatsphäre der Google-Nutzer ein. Google wird außerdem verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, die sicherstellen, dass die Google-Nutzer künftig selbst über die Verwendung ihrer Daten zur Profilerstellung entscheiden können.

Während nach deutschem Datenschutzrecht eine Verwaltungsanordnung erlassen wurde, konnten andere Länder aufgrund ihrer nationalen Bestimmungen die Verstöße mit Bußgeldern sanktionieren. So hatte die spanische Datenschutzbehörde AEPD im Dezember 2013 gegen Google eine Geldstrafe in Höhe von 900.000 Euro verhängt. Ebenso die französische Aufsichtsbehörde CNIL, die Anfang 2014 eine Strafzahlung in Höhe von 150.000 Euro anordnete. In den Niederlanden wurde sogar eine Geldbuße von bis zu 15 Millionen Euro angedroht, wenn Google nicht den dortigen Auflagen der Datenschutzbehörde CBP nachkommt und von seinen Nutzern die Einwilligung einholt, damit die Daten aus verschiedenen Diensten wie z. B. der Websuche, mobilen Diensten, Google Mail und YouTube für Werbezwecke miteinander kombiniert werden dürfen. Die Nutzer sollen auch deutlich darüber aufgeklärt werden, welche Daten von diesen Diensten genutzt werden.

Der Widerspruch, den Google gegen die Verwaltungsanordnung eingelegt hatte, wurde im April 2015 vom HmbBfDI abschließend beschieden. Zwar wurde die Anordnung aufgrund rechtsförmlicher Einwände angepasst, in der Hauptsache wurde der Widerspruch jedoch zurückgewiesen. Gegen diese Anordnung hat Google eine Anfechtungsklage vor dem Verwaltungsgericht Hamburg erhoben. Allerdings wurde bereits seitens Google signalisiert, dass substantielle Änderungen an den Diensten erfolgen sollen, um die Anforderungen des Datenschutzrechts zu erfüllen. Es besteht also die Hoffnung, dass die gemeinsamen Anstrengungen der europäischen Datenschutzaufsichtsbehörden Wirkung zeigen.

5.12 Suchmaschinen und das „Recht auf Vergessen“

5.12.1 Das EuGH-Urteil

Der EuGH hat in seinem Urteil vom 13. Mai 2014 (Az. C131/12; NJW 2014, 2257) festgestellt, dass Privatpersonen ein direkter Löschungsanspruch gegen Suchmaschinenbetreiber hinsichtlich Links zustehe, die ihre Person betreffen. Der Betreiber einer Suchmaschine sei bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich. Künftig sind die Betroffenen daher nicht mehr darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Webseitenbetreibern zu verfolgen, die Informationen zu ihrer Person veröffentlichen. Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche nach ihrem Namen einzelne Links künftig nicht mehr angezeigt werden.

Grundlage für die Entscheidung war der Fall eines Spaniers, der 1998 im Zusammenhang mit einer Immobilienpfändung namentlich in einer Zeitung genannt wurde. Das Archiv der Zeitung wurde digitalisiert und war somit im Internet bei Google zu finden. Der Betroffene beschwerte sich bei der spanischen Datenschutzkommission, die ihm Recht gab. Google klagte gegen die Entscheidung beim spanischen Obergericht, das im nächsten Schritt eine Auslegung der EU-Datenschutzrichtlinie vom EuGH forderte.

Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben, da sich damit weltweit detaillierte Profile von Personen erstellen lassen. Oft sind die Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert werden.

Die Entfernung von Links aus der Ergebnisliste kann sich aber auf das berechtigte Interesse von potenziell am Zugang zu der Information interessierten Internetnutzern auswirken. Nach Ansicht des EuGH sei daher ein angemessener Ausgleich zwischen diesem Interesse und den Grundrechten der betroffenen Person, insbesondere des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten, zu finden. Es geht also immer um die Abwägung zwischen der Privatsphäre des Betroffenen und dem Interesse der Allgemeinheit an einer Information, wobei das Ergebnis der Abwägung auch davon abhängt, ob es sich um eine Privatperson oder eine Person des öffentlichen Lebens handelt.

Zur Unterstützung bei Fragen der Löschung von Suchergebnissen hat Google im Juli 2014 einen Experten-Beirat einberufen, dem u. a. die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger angehört. Der Löschbeirat hat von verschiedenen Gruppen Stellungnahmen eingeholt und in mehreren europäischen Städten getagt, in denen Experten angehört wurden. Auf dieser Basis und nach weiteren internen Beratungen wurde Anfang Februar 2015 ein Bericht zum "Recht auf Vergessenwerden“ vorgelegt. Darin plädieren die Experten mehrheitlich dafür, Anträge auf Löschungen großzügiger zu handhaben. Bisher wurden sechzig Prozent der 205 000 Löschanträge, die Bürger in Europa seit dem Urteil des EuGH gestellt haben, abgelehnt. Außerdem empfiehlt der Beirat, das Antragsformular zu konkretisieren und den betroffenen Seitenbetreiber nicht über die Löschung der Links zu informieren, da dies einer erneuten Verletzung der Privatsphäre gleichkäme.

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2014 eine Entschließung verabschiedet (**Anlage 15**). Darin wird auch gefordert, dass angesichts der territorialen Unbeschränktheit des Internets der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten muss. Deshalb beinhaltet die effektive Wahrung der Persönlichkeitsrechte des Betroffenen, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit zu sperren haben.

5.12.2 Hinweise zur Löschung von Google-Einträgen

Möchten Betroffene Suchergebnisse zu ihrem Namen löschen lassen, müssen sie ihr Löschbegehren zunächst direkt an Google[7] richten. Dazu muss das dort beschriebene Verfahren durchgeführt bzw. das dortige Formular[8] ausgefüllt werden. Zur Authentifizierung ist es nicht erforderlich, amtliche Ausweiskopien an Google zu übermitteln. Es ist ausreichend, andere Nachweise wie z. B. Bibliotheksausweise o. ä. zu

[7] https://support.google.com/legal/

[8] https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de

verwenden und nicht erforderliche Angaben zu schwärzen. Insbesondere braucht das Dokument kein Foto des Antragstellers zu enthalten.

Sollte Google die Löschung der Suchergebnisse ablehnen, können sich die Betroffenen an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden, da dieser als Datenschutzaufsichtsbehörde für die deutsche Niederlassung von Google zuständig ist.

Dieser ist unter folgender Adresse erreichbar:

> Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
> Klosterwall 6 (Block C), 20095 Hamburg
> Tel.: (040) 4 28 54 - 40 40
> Fax: (040) 4 28 54 - 40 00
> E-Mail: mailbox@datenschutz.hamburg.de

Für eine erfolgreiche Bearbeitung der Eingabe ist es erforderlich, dass neben der Nennung des Suchbegriffes und des konkreten Links die bisher geführte Kommunikation und die Bearbeitungsnummer (Ticketnummer), die der Betroffene durch den Kundensupport von Google erhalten hat, übersendet wird.

Unabhängig von dem oben beschriebenen Vorgehen sollten die Betroffenen versuchen, soweit dies nicht bereits geschehen ist, die beanstandeten Informationen oder Daten in den Originalquellen löschen zu lassen. Dies erschwert dann auch die Verbreitung der Daten über andere Suchmaschinen und Internetdienste.

5.13 Bewertungsportale

Bewertungsportale im Internet erfreuen sich großer Beliebtheit. Dort kann man Loben oder seinem Unmut Luft machen und sich ohnehin informieren. Was von den einen gern genutzt wird, führt aber bei den anderen oft zu Verdruss. Sie beklagen, dass zu ihrer Person negative Äußerungen veröffentlicht werden. Zumeist ist es nur schwer möglich, diese zu korrigieren. Der Bundesgerichtshof hatte schon am 23. Juni 2009 in einem Urteil zu einem Lehrerbewertungsportal (Az. VI ZR 196/08, juris) entschieden, dass kein Löschungsanspruch der Betroffenen besteht, wenn nicht die Grenze der Schmähkritik bzw. der Formalbeleidigung überschritten wird. Die Anonymität der Bewertenden ist durch die Meinungsfreiheit des Grundgesetzes gewährleistet. Der Landesbeauftragte hatte hierzu bereits im IX. Tätigkeitsbericht (Nr. 20.6) berichtet. Die Datenschutzaufsichtsbehörden haben sich mit der Thematik weiter befasst und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Leitlinien für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet beschlossen. Der Landesbeauftragte beobachtet die Entwicklung weiter.

In neueren Entscheidungen hat der Bundesgerichtshof einen Anspruch auf Auskunft über Nutzer eines Arztbewertungsportals verneint, da der Betreiber für die Herausgabe der Nutzerdaten nicht die nach § 12 Abs. 2 TMG geforderte Rechtsgrundlage habe (Urteil vom 1. Juli 2014, Az. IX ZR 345/13, openjur.de). Mit Urteil vom 23. September 2014 (Az. VI ZR 358/13, juris) bestätigte der Bundesgerichtshof, dass ein in seiner Sozialsphäre betroffener Arzt gegen den Betreiber eines Arztbewertungsportals grundsätzlich keinen Anspruch auf Löschung hat. Dem stehen die Interessen des Betreibers infolge der grundrechtlich geschützten Berufs-, Kommunikations- und

Meinungsfreiheit entgegen. Der Arzt ist jedoch nicht schutzlos, da er gegebenenfalls die Beseitigung von unwahren Tatsachenbehauptungen und beleidigenden oder sonst unzulässigen Bewertungen verlangen und zivilrechtlich durchsetzen kann.

5.14 Recht am eigenen Bild bei Kindern und Jugendlichen

Mehrfach war der Landesbeauftragte mit Beschwerden befasst, die das Recht am eigenen Bild von Kindern und Jugendlichen betrafen. Dabei ging es um die Frage, ob bei Ferienveranstaltungen Fotografien angefertigt und diese auf Internetseiten sozialer Medien veröffentlicht werden dürfen. Zusätzlich war zu klären, ob diejenigen Kinder und Jugendlichen von der Teilnahme ausgeschlossen werden können, die selbst (oder deren Eltern) keine derartige Veröffentlichung wollen.

Das Recht am eigenen Bild wird unmittelbar aus dem allgemeinen Persönlichkeitsrecht hergeleitet. Es wird insbesondere durch die §§ 22, 23 und 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) geschützt. Soweit diese Vorschriften anwendbar sind, gehen sie als bereichsspezifische Vorschriften dem BDSG vor (§ 1 Abs. 3 Satz 1 BDSG).

Grundsätzlich dürfen Bildnisse nach § 22 KunstUrhG nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Ausnahmen davon enthält § 23 KunstUrhG für

- Bildnisse aus dem Bereich der Zeitgeschichte,
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen,
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben,
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

Die Befugnis erstreckt sich jedoch nicht auf die Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten verletzt wird.

Vor diesem Hintergrund war eine Veröffentlichung von Bildnissen der Teilnehmer der Ferienveranstaltungen insbesondere auf Internetseiten sozialer Medien ohne deren Einwilligung nicht zulässig. Zwar mag es sein, dass ein größere Ferienveranstaltung dem Bereich der Zeitgeschichte zuzuordnen ist. Der Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinem gesellschaftlichem Interesse. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören (BGH, NJW-RR 2014, 1193-1195). Allerdings ist das Informationsinteresse der verantwortlichen Stelle nach dem Grundsatz der Verhältnismäßigkeit mit dem Recht am eigenen Bild der Abgebildeten abzuwägen. Soweit ein Ereignis von lokaler Bedeutung anzunehmen wäre, müssten Veröffentlichungen sich auf diesen Bedeutungsumfang beschränken. Damit könnte die Veröffentlichung von Bildnissen der Teilnehmer in diesem Rahmen gerechtfertigt sein, wenn auf den jeweiligen Fotografien die Dokumentation der Veranstaltung im Vordergrund steht und Personen nicht unvorteilhaft oder ehrverletzend dargestellt werden.

Eine Veröffentlichung im Internet wäre damit nicht zulässig. Besonders problematisch wäre eine Veröffentlichung auf Internetseiten sozialer Netzwerke, bei denen der Betreiber des Netzwerks in seinen allgemeinen Geschäftsbedingungen erklärt, dass die Rechte an Fotografien an ihn abgetreten werden. So heißt es z. B. in den „Unternehmensinformationen“ von Facebook: *„Für Inhalte, die durch Rechte am geistigen Eigentum geschützt sind, wie Fotos und Videos (IP-Inhalte), erteilst du uns ausdrücklich nachfolgende Genehmigung, vorbehaltlich deiner Einstellungen für Privatsphäre und Apps: Du gewährst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jedweder IP-Inhalte, die du auf bzw. im Zusammenhang mit Facebook postest (IP-Lizenz).“* Unabhängig davon, ob eine derartige Klausel rechtlich wirksam ist, verlieren Abgebildete und auch die verantwortliche Stelle de facto jede Möglichkeit, ein einmal gepostetes Bildnis aus dem Internet zu entfernen.

Die Veröffentlichung im Internet hätte im hier vorliegenden Fall damit eine Einwilligung nach § 22 KunstUrhG verlangt. Bei Minderjährigen muss die Einwilligung stets bei den Personensorgeberechtigten eingeholt werden. Ob zusätzlich eine Einwilligung der Jugendlichen eingeholt werden muss, hängt von deren Einwilligungsfähigkeit ab. Jugendliche sind dann einwilligungsfähig, wenn sie die Risiken, die mit einer Veröffentlichung des Bildnisses entstehen, einschätzen können. Hier ist zwar keine starre Altersgrenze anzunehmen. Der Landesbeauftragte empfiehlt jedoch, die Einwilligung des Jugendlichen spätestens ab dem 14. Lebensjahr einzuholen. Unterhalb dieser Altersgrenze dürfte bei Veröffentlichungen im Internet regelmäßig die Einwilligung der Personensorgeberechtigten ausreichen.

Die Einwilligung sollte grundsätzlich schriftlich erfolgen. Es ist anzugeben, zu welchem Zweck die Bildnisse gefertigt werden sollen. Insbesondere sollte genau ausgeführt werden, in welchen Medien (Zeitung, Homepage des Veranstalters, soziale Medien) sie veröffentlicht werden. Hinzuweisen ist auch auf die Risiken, die mit einer Veröffentlichung im Internet verbunden sind (nichtberechtigte Nutzung durch Dritte, Veränderbarkeit, weltweite Abrufbarkeit). Idealerweise sollte dem Betroffenen bzw. seinen Personensorgeberechtigten das jeweilige Bildnis zur Einwilligung vorgelegt werden.

Ein Ausschluss der Teilnehmer, die selber oder deren Personensorgeberechtigten keine Einwilligung zur Veröffentlichung der Bildnisse im Internet erteilen, begegnet erheblichen Bedenken. Hier sollte bedacht werden, dass zu Ferienveranstaltungen, wie z. B. Sommercamps, in dem örtlichen Bereich, in dem sie stattfinden, häufig keine Alternativen bestehen. Daher werden auch Interessenten, die nicht gänzlich mit der Veröffentlichung einverstanden sind, u. U. geneigt sein, eine Anmeldung zu unterschreiben. Die mit der Anmeldung erklärte Einwilligung entspricht hier nicht dem wahren Willen der Betroffenen.

Die oben genannten Gesichtspunkte wurden mit der verantwortlichen Stelle, die die Ferienveranstaltungen durchführte, erörtert. Im Ergebnis sollten nur Bilder veröffentlicht werden, zu denen eine Einwilligung vorlag. Zudem wurde von der Absicht, eine Einwilligungserklärung zur Veröffentlichung der Bilder im Internet als Teilnahmevoraussetzung festzusetzen, abgesehen.

6 Öffentliche Sicherheit, Meldewesen

6.1 SOG LSA

In seinem XI. Tätigkeitsbericht (Nr. 5.1) hat der Landesbeauftragte ausführlich das Verfahren zur Änderung des SOG LSA im Jahr 2013 beschrieben. Letztendlich trat das Gesetz zur Neuregelung und Erhebung von telekommunikations- und telemedienrechtlichen Bestandsdaten, als dessen Art. 1 die Änderung des SOG LSA erfolgte, am 10. Oktober 2013 in Kraft (GVBl. LSA S. 494). Aus datenschutzrechtlicher Sicht konnte der Landesbeauftragte mit den Regelungen nicht vollends zufrieden sein, obwohl Anregungen Berücksichtigung fanden.

Bedenken hatte der Landesbeauftragte in Bezug auf Regelungen des SOG LSA bereits zur vorherigen Novelle (GVBl. LSA S. 145) geäußert. Mit dem Vierten Gesetz zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung wurden Regelungen eingeführt, die auch unter datenschutzrechtlichen Aspekten betrachtet, nicht alle als vertretbar angesehen werden konnten. Hinsichtlich der Bedenken im Einzelnen wird auf den XI. Tätigkeitsbericht (Nr. 5.1) verwiesen.

Dieses Vierte Änderungsgesetz hatten Abgeordnete der Fraktionen Die Linke und Bündnis90/Die Grünen im Rahmen eines Normenkontrollantrages durch das Landesverfassungsgericht einer Überprüfung unterziehen lassen. Sie vertraten die Auffassung, dass Teile des Änderungsgesetzes verfassungswidrig seien und bestehende Befugnisse der Polizei deutlich zu Lasten der Grundrechte der Bürgerinnen und Bürger erweitert worden. Konkret sollte die Zulässigkeit der Neuregelungen zur Anfertigung von Videoaufzeichnungen bei polizeilichen Kontrollen im Straßenverkehr (§ 16 Abs. 3 SOG LSA), zur Erhebung von Telekommunikationsinhalten und Telekommunikationsumständen (§ 17b SOG LSA), zur Erhebung von Telekommunikationsinhalten und Telekommunikationsumständen in informationstechnischen Systemen (§ 17c SOG LSA), zur Unterbrechung und Verhinderung von mobilen Kommunikationsverbindungen (§ 33 SOG LSA), zur zwangsweisen Untersuchung von Personen bei Verdacht auf Übertragung besonders gefährlicher Krankheitserreger (§ 41 Abs. 6 SOG LSA) sowie zu Alkoholgefahren (§ 94a SOG LSA) überprüft werden.

Am 11. November 2014 hat das Landesverfassungsgericht Sachsen-Anhalt sein Urteil (LVG 9/13, NVwZ 2015, 438) im Normenkontrollverfahren verkündet. Zusammenfassend lässt sich feststellen, dass § 17c SOG LSA für nichtig erklärt wurde, dass § 94a SOG LSA ebenfalls verfassungswidrig ist, dass §§ 16 Abs. 3, 17b und 41 Abs. 6 SOG LSA nach Maßgabe des Urteils weiterhin anwendbar sind, der Gesetzgeber aber bis zum 31. Dezember 2015 verfassungskonforme Neuregelungen zu schaffen hat und dass § 33 SOG LSA durch das Landesverfassungsgericht Sachsen-Anhalt bestätigt wurde.

Aus datenschutzrechtlicher Sicht von besonderem Interesse ist die Begründung zur Verfassungswidrigkeit der Regelungen zur Erhebung von Telekommunikationsinhalten und Telekommunikationsumständen in informationstechnischen Systemen, besser bekannt als Quellen-Telekommunikationsüberwachung (§ 17c SOG LSA). Das Landesverfassungsgericht Sachsen-Anhalt führt insoweit aus:

„Obwohl der Gesetzgeber mit dem Schutz von Leib, Leben oder Freiheit einer Person in Fällen einer gegenwärtigen Gefahr einen legitimen und zugleich ausreichend

gewichtigen Zweck verfolgt, ist die getroffene Regelung zum derzeitigen Zeitpunkt und in der vorliegenden Form unverhältnismäßig, weil der Gesetzgeber keine verantwortliche Abwägungsentscheidung getroffen hat. Das ergibt sich aus dem in der mündlichen Verhandlung durch die Landesregierung bestätigten Umstand, dass es bislang noch keine technischen Mittel gibt, um die Norm umzusetzen. Der Gesetzgeber hat demnach die Polizei zu Maßnahmen und zum Einsatz von (technischen) Instrumenten ermächtigt, die er noch gar nicht kennen und bewerten konnte, weil es sie gar nicht gibt. Damit fehlt aber eine durch den Gesetzgeber verantwortete Abwägung, die für eine grundrechtsbeschränkende Maßnahme unverzichtbar ist.

Daran ändert auch der Umstand nichts, dass der Gesetzgeber allgemeine Vorgaben für den Einsatz der technischen Mittel in Absatz 3 formuliert hat. Diese alleine führen nicht dazu, dass er selbst eine Abwägungsentscheidung unter Berücksichtigung der Leistungsfähigkeit der eingesetzten Instrumente und ihrer Grenzen treffen konnte. Bereits die Formulierung „es ist technisch sicherzustellen“ in Absatz 3 am Anfang sowie die mehrfache Bezugnahme auf das „technisch Mögliche“ machen deutlich, dass der Gesetzgeber nur sehr vage Vorstellungen davon hatte, was technisch möglich ist und welche Abstriche am Schutz von Vertraulichkeit der erhobenen Informationen sowie des Zugriffs auf andere Inhalte, die nicht vom Zweck der Norm erfasst sind, hinzunehmen sind.

In einer solchen Situation der Ungewissheit muss der Gesetzgeber entweder auf eine Regelung von Eingriffsbefugnissen verzichten oder einen von ihm ausgestalteten und parlamentarisch kontrollierbaren Entscheidungsprozess über die „Zulassung“ der technischen Instrumente in die gesetzliche Regelung integrieren. Ein blindes Vertrauen darauf, dass die Exekutive nur die den allgemeinen Vorgaben „entsprechenden“ Instrumente einsetzt, reicht in einer solchen Situation der Unwissenheit nicht aus, um eine verantwortbare Abwägung und Entscheidung zu treffen.

Aus diesem Grunde erweist sich die in § 17c SOG LSA getroffene Regelung jedenfalls zum jetzigen Zeitpunkt als verfassungswidrig und nichtig.“

Die Kernaussagen des Landesverfassungsgerichtes Sachsen-Anhalt, dass eine gesetzliche Regelung verfassungskonform nur getroffen werden kann, wenn

1. der Gesetzgeber in Kenntnis bestehender technischer Möglichkeiten eine verantwortliche Abwägungsentscheidung treffen kann oder

2. der Gesetzgeber einen von ihm ausgestalteten und parlamentarisch kontrollierbaren Entscheidungsprozess über die „Zulassung“ der technischen Instrumente in die gesetzliche Regelung integriert und dass

3. er diesen Prozess nicht im Vorgriff auf ggf. in Zukunft bestehende technische Möglichkeiten der Exekutive übertragen kann,

werden zukünftig wohl nicht nur der Maßstab bei der Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung sein. Vielmehr werden sich an diesen Maßstäben alle rechtlichen Grundlagen messen lassen müssen, aufgrund derer mit technischen Mitteln Grundrechtseingriffe ermöglicht werden sollen (siehe bereits X. Tätigkeitsbericht Nr. 1.1).

Der Gesetzgeber hat mit einem Fünften Änderungsgesetz ausschließlich die Vorgaben des Landesverfassungsgerichtes umgesetzt (GVBl. LSA 2015 S. 559). Zu einer weitergehenden datenschutzfreundlicheren Reform kam es nicht.

6.2 Risikomanagement für besonders rückfallgefährdete Sexualstraftäter

In seinem XI. Tätigkeitsbericht (Nr. 5.4) hat der Landesbeauftragte über den Erlass zur Einrichtung von RiMS-LSA, dem Risikomanagement für besonders rückfallgefährdete Sexualstraftäter im Land Sachsen-Anhalt, berichtet. Mit der letztendlich schlussgezeichneten und im April 2013 veröffentlichen Fassung (MBl. LSA 2013 S. 207) des Erlasses waren jedoch nicht alle Bedenken des Landesbeauftragten ausgeräumt.

Im August 2013 wurde der Landesbeauftragte durch das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt darüber unterrichtet, dass es für die Erfüllung der Aufgaben der Polizei notwendig sei, alle zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung oder Vorsorge für die Verfolgung von Straftaten erforderlichen personenbezogenen Daten zu einem Probanden sowie weiterer Personen übersichtlich, aufgabenbezogen und strukturiert vorzuhalten sowie alle in diesem Zusammenhang erfolgten behördlichen Maßnahmen zu dokumentieren. Zu diesem Zweck sei es erforderlich, ein automatisiertes Verfahren einzuführen, welches es den Mitarbeitern der Gemeinsamen Zentralstelle beim Landeskriminalamt bzw. des Fachkoordinatoren der Polizeidirektionen ermögliche, ihre ihnen nach der Erlasslage obliegenden Aufgaben sach- und zeitgerecht zu erfüllen. Insbesondere diene das Verfahren dazu, die erforderlichen Datenübermittlungen zur Abwehr einer gegenwärtigen erheblichen Gefahr zeitgerecht zu ermöglichen.

Nach Prüfung des für dieses automatisierte Verfahren übersandten Entwurfes für ein Verfahrensverzeichnis hat der Landesbeauftragte mit seiner Stellungnahme gegenüber dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt nochmals deutlich gemacht, dass es datenschutzrechtlich nicht vertretbar sei, in einer Gemeinsamen Zentralstelle für Polizei und Justiz eine Datensammlung vorzuhalten, die alle Erkenntnisse zu einer bestimmten Person bündelt und auf die sowohl Polizei als auch Justiz Zugriff haben. Hintergrund ist, dass die Polizei nur Zugriff auf die Daten haben darf, die sie zur Erfüllung ihrer polizeilichen Aufgaben benötigt. Die Justiz wiederum darf nur auf Daten zugreifen, die sie zur Erledigung ihrer, sich von denen der Polizei grundlegend unterscheidenden, Aufgaben benötigt.

Das vorgelegte Verfahrensverzeichnis stellte auf diese bereits früher geltend gemachten Bedenken insoweit ab, als nunmehr zwar ein automatisiertes Verfahren eingerichtet, dieses aber lediglich von der Polizei genutzt werden solle. Die Frage nach einer Vermischung personenbezogener Daten von Polizei und Justiz in einer Datensammlung war damit zwar zunächst geklärt, die Erforderlichkeit einer solchen Datensammlung an sich aber nicht hinreichend belegt.

Die Übersendung einer anschließend erneut überarbeiteten Fassung des Verfahrensverzeichnisses und eine weitergehende Erläuterung zu Fragen der Erforderlichkeit durch das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt haben den Landesbeauftragten letztendlich dazu bewogen, unter Zurückstellung bestehender datenschutzrechtlicher Bedenken keine weiteren Einwände zu erheben.

6.3 Öffentlichkeitsfahndung in sozialen Netzwerken

In seinem XI. Tätigkeitsbericht (Nr. 5.6) hat der Landesbeauftragte zur Öffentlichkeitsfahndung in sozialen Netzwerken ausgeführt, dass es sich dabei und bei der Nutzung sozialer Netzwerke für Aufgaben der Polizei um eine grundlegende Entwicklung handelt, die auch an Sachsen-Anhalt nicht vorbei geht bzw. gehen wird. Die Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht (LT-Drs. 6/3512) beschränkte sich darauf festzustellen, dass soziale Netzwerke im Berichtszeitraum in Sachsen-Anhalt nicht zur Öffentlichkeitsfahndung genutzt wurden.

Obwohl dies nach Kenntnis des Landesbeauftragten für Sachsen-Anhalt bis heute zutrifft, hat er sich als Mitglied der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus Anlass ihrer Tagung im März 2014 den rechtlichen Problemstellungen einer solchen Nutzung gewidmet. Im Ergebnis der Beratungen hat die Konferenz die Entschließung „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“ (**Anlage 8**) gefasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wies mit ihrer Entschließung darauf hin, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Die Konferenz führt weiter aus, dass, sofern es Strafverfolgungsbehörden trotz bestehender datenschutzrechtlicher Bedenken gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke zurückzugreifen, dies nur unter bestimmten Maßgaben vorstellbar wäre. Die insoweit aus Sicht der Konferenz erforderlichen Maßgaben hat sie in ihrer Entschließung ausdrücklich benannt.

Die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat der Landesbeauftragte der Justizministerin und dem Innenminister Sachsen-Anhalts jeweils mit der Bitte übersandt, über die aktuellen Diskussionsstände in der Justiz- bzw. Innenministerkonferenz zu informieren. Aufgrund der vorliegenden Schreiben aus beiden Häusern ist dem Landesbeauftragten bekannt, dass die Öffentlichkeitsfahndung in sozialen Netzwerken in Sachsen-Anhalt nach wie vor nicht durchgeführt wird. Es ist aber eine Änderung der Anlage B zu den Richtlinien für das Straf- und Bußgeldverfahren beabsichtigt, der zufolge diese Art der Fahndung ermöglicht wird. Problematisch ist der Umstand, dass Staatsanwaltschaften und Polizeibehörden ein öffentliches Diskussionsforum eröffnen können; zumal bei Facebook die Kommentierungsfunktion nicht abschaltbar ist.

6.4 GIAZ – Teil IV

Zuletzt hatte der Landesbeauftragte in seinem X. Tätigkeitsbericht (Nr. 26.3) über das GIAZ – damals noch das „Gemeinsame Informations- und Auswertungszentrum islamistischer Terrorismus“ – berichtet. Seither ist viel geschehen, was den Charakter des Zentrums grundlegend verändert hat. Die Abkürzung GIAZ ist zwar geblieben, ihre Bedeutung allerdings nicht. Heute ist das GIAZ ein „Gemeinsames Informations- und Abwehrzentrum im Landeskriminalamt Sachsen-Anhalt“.

Dass der Landesbeauftragte insbesondere mit Blick auf die Einhaltung des Trennungsgebotes stets Bedenken gegen die Ausgestaltung der Zusammenarbeit zwischen Polizei und Verfassungsschutz im GIAZ hatte, hat er in vielfacher Form gegenüber dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt vertreten und in drei Beiträgen in seinen Tätigkeitsberichten dokumentiert. Diese Bedenken konnten nach wie vor nicht ausgeräumt werden.

Ende Februar 2014 wurde der Landesbeauftragte durch das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt unterrichtet, dass der bis dahin geltende Erlass, der die Aufgaben des GIAZ näher definierte und die Form der Zusammenarbeit im GIAZ regelte, überarbeitet werden soll. Die Änderungen seien den Erkenntnissen in Auswertung des NSU-Komplexes durch eine Experten-Kommission und einen Bundestagsuntersuchungsausschuss geschuldet. Die „Ständige Konferenz der Innenminister und -senatoren der Länder“ habe Beschlüsse in Umsetzung der Empfehlungen dieser Gremien gefasst, die es auch in Sachsen-Anhalt umzusetzen gelte. Im neuen GIAZ sollten nunmehr phänomenübergreifend und im Sinne eines ganzheitlichen Bekämpfungsansatzes alle relevanten Erkenntnisse zu Personen, Objekten und Sachen an einer Stelle aufbereitet, bewertet und den jeweiligen Bedarfsträgern zugeleitet werden. Insoweit würde das GIAZ von einem Auswertungs- zu einem Abwehrzentrum umgestaltet. Diesen Ausführungen war der Entwurf des geänderten Erlasses mit dem Hinweis beigefügt, dass ein Inkrafttreten zum 1. März 2014 vorgesehen sei. Wegen der Kurzfristigkeit der Unterrichtung hat der Landesbeauftragte das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt noch im Februar 2014 darauf hingewiesen, dass derartige Fristsetzungen keinesfalls dem Sinn der Unterrichtungspflicht nach § 14 Abs. 1 Satz 3 DSG LSA entsprechen, die auf eine rechtzeitige Unterrichtung abstellt, und nur eine summarische Prüfung vorgenommen werden konnte. Der Landesbeauftragte trug inhaltlich vor, dass sich die veränderte Ausrichtung des GIAZ aus dem Erlass nicht erschließen lasse, dass einzelne Aufgabenbeschreibungen der Erklärung bedürfen und dass in Bezug auf die Einhaltung des Trennungsgebotes das Urteil des Bundesverfassungsgerichtes zur Antiterrordatei vom 24. April 2013 (1 BvR 1215/07) mit dem darin beschriebenen informationellen Trennungsprinzip einzubeziehen sei.

Aufgrund wiederholter Nachfragen im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt brachte der Landesbeauftragte in Erfahrung, dass vom Inkraftsetzen des Erlasses zum März 2014 abgesehen wurde und eine erneute Überarbeitung vorgesehen sei. Zum Bearbeitungsstand erkundigte sich der Landesbeauftragte regelmäßig.

Erst Ende November 2014 unterrichtete das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt den Landesbeauftragten schriftlich von der nunmehr abgeschlossenen Überarbeitung des Erlassentwurfes und dem Entwurf eines weiteren Erlasses, der die Datenübermittlungen zwischen Polizei und Verfassungsschutz regeln soll. Der Erlass zum GIAZ stellte sich als grundlegend überarbeitet dar, der Erlass zur Datenübermittlung lag erstmalig vor. Dennoch teilte das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt mit, dass es nunmehr beabsichtige, die Erlasse zum 1. Januar 2015 in Kraft zu setzen.

Mit diesem Schreiben wurde nunmehr deutlich, dass im GIAZ künftig alle Facetten der politisch motivierten Kriminalität berücksichtigt werden sollen. Das bis dahin lediglich für den Bereich des islamistischen Terrorismus zuständige GIAZ solle auch

die Bereiche Rechtsextremismus/-terrorismus, Linksextremismus/-terrorismus, Ausländerextremismus/-terrorismus und Spionage/Proliferation abdecken. Zentrale Aufgabe des GIAZ sei es dabei, die Zusammenarbeit der Polizei des Landes Sachsen-Anhalt mit den entsprechend auf Bundesebene eingerichteten Terrorismusabwehrzentren, über die der Landesbeauftragte in seinem XI. Tätigkeitsbericht (Nr. 5.3) berichtet hat, sicherzustellen.

Im Dezember 2014 hat der Landesbeauftragte das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt wiederum darauf aufmerksam gemacht, dass eine eingehende Prüfung der Unterlagen, wie sie im Rahmen einer Unterrichtung nach § 14 Abs. 1 Satz 3 DSG LSA erforderlich ist, aufgrund der Zeitvorgaben nicht möglich ist. Erst daraufhin wurde dem Landesbeauftragten eine Frist zur Stellungnahme bis Ende Januar 2015 eingeräumt.

Mit seiner Stellungnahme vom Januar 2015 musste der Landesbeauftragte trotz der vorgenommenen Überarbeitung feststellen, dass seine Bedenken hinsichtlich der Einhaltung des Trennungsgebotes nicht ausgeräumt werden konnten. Mit Blick auf den veränderten Charakter des GIAZ vom Auswertungs- zum Abwehrzentrum besteht die Gefahr, dass die vorgesehene Abstimmung von Maßnahmen bezogen auf die Verfassungsschutzbehörde den Übergang zu einem operativen Handeln bedeuten kann. Ein solches wäre aber nicht vom gesetzlich definierten Aufgabenbereich des Verfassungsschutzes gedeckt. Bezüglich des Erlassentwurfes zur Datenübermittlung stellten sich dem Landesbeauftragten auch Fragen nach der Anwendbarkeit bestimmter Rechtsgrundlagen, auf die sich der Erlass bezieht.

Dem Landesbeauftragten wurde bis zum Jahresende 2015 keine überarbeitete Fassung zugeleitet. Die ursprünglich geltend gemachte Dringlichkeit scheint nicht mehr gegeben zu sein.

6.5 Meldewesen

6.5.1 Bundesmeldegesetz

Bereits in seinem X. Tätigkeitsbericht (Nr. 6.3) und in seinem XI. Tätigkeitsbericht (Nr. 5.9.1) hatte der Landesbeauftragte über den Gesetzentwurf zur Fortentwicklung des Meldewesens berichtet und einen Ausblick auf die Neuregelung des Meldewesens gegeben, wonach das bisherige Melderechtsrahmengesetz und das Landesmeldegesetz durch das Bundesmeldegesetz (BMG) abgelöst werden.

Noch bevor das BMG in Kraft treten sollte, wurde es bereits geändert. Während die Vorschriften zu Regelungsbefugnissen der Länder, zu Verordnungsermächtigungen des Bundes und zum Erlass von Verwaltungsvorschriften des Bundes (§§ 55 bis 57 BMG) bereits zum 26. November 2014 in Kraft getreten sind, sollten die übrigen Regelungen zum 1. Mai 2015 in Kraft treten. Es stellte sich jedoch frühzeitig heraus, dass die den Landesgesetzgebern zugewiesenen Regelungsbefugnisse nicht zeitnah, also gleichzeitig mit dem Bundesmeldegesetz umgesetzt werden konnten. Der Zeitpunkt des Inkrafttretens wurde auf den 1. November 2015 festgesetzt (BGBl. I S. 1738).

Aus datenschutzrechtlicher Sicht wird begrüßt, dass der Bundesgesetzgeber in diesem Zusammenhang die in § 10 BMG normierten Auskunftsrechte der Betroffenen klarer formulierte. Künftig erhalten Betroffene im Einzelfall auf Antrag auch Auskunft über die Arten der übermittelten Daten und ihre Empfänger bei automatisierten Melderegisterauskünften.

6.5.2 Entwurf eines Ausführungsgesetzes des Landes zum Bundesmeldegesetz

Im August 2014 übersandte das Ministerium für Inneres und Sport einen Entwurf eines Ausführungsgesetzes des Landes Sachsen-Anhalt zum Bundesmeldegesetz und zur Regelung der Zuständigkeit im Personalausweisrecht.

Der Landesbeauftragte konnte dem Anliegen des Landesgesetzgebers, die erforderlichen landesrechtlichen Regelungen an die neue Rechtslage im Melde- und Ausweisrecht anzupassen, grundsätzlich folgen. Er stellte jedoch klar, dass insbesondere der Aufbau eines zentralen Meldedatenbestandes für die automatisierten Behördenabrufe (siehe Nr. 6.5.3) neben den originären Melderegistern der Kommunen aus datenschutzrechtlicher Sicht differenziert gesehen werde. Einerseits enthält der Zentrale Meldedatenbestand nicht alle Daten, Hinweise und Ordnungsmerkmale des Bundesmeldegesetztes, was aus datenschutzrechtlichen Gesichtspunkten begrüßt wird. Andererseits wird durch den Aufbau eines Zentralen Meldedatenbestandes ein „Spiegelregister“ eingeführt, das neben den Melderegistern der Meldebehörden geführt wird. Die Schaffung einer zusätzlichen Struktur auf Landesebene wird unter dem Gebot der Datenvermeidung und Datensparsamkeit aber auch unter dem Verbot der Datenvorratshaltung kritisch gesehen.

Im Gesetzentwurf wurde deutlich, dass dazu eine Landesinformationsstelle – nämlich Dataport in Hamburg (vgl. Nr. 4.6) – eigenverantwortliche Aufgaben nach dem Bundesmeldegesetz wahrnehmen soll, während die Fachaufsicht auf das für das Melderecht zuständige Ministerium übertragen wurde. Es sprach einiges dafür, dass anstelle einer Auftragsdatenverarbeitung nach § 8 DSG LSA der Landesinformationsstelle durch Funktionsübertragung eigenverantwortliche Aufgaben übertragen werden sollten. Der Landesbeauftragte wies daraufhin, dass dann die Landesinformationsstelle Meldebehörde im Sinne des Gesetzentwurfes werde, welches auch im Gesetzesentwurf deutlich aufgezeigt werden müsse.

Unter dem Gesichtspunkt der eigenverantwortlichen Wahrnehmung von Aufgaben durch die Landesinformationsstelle als Meldebehörde kritisierte der Landesbeauftragte zusätzlich, dass diese ihren Sitz – unabhängig von ihren Außenstellen in Magdeburg und Halle – außerhalb von Sachsen-Anhalt hat, was zumindest für klärungsbedürftig gehalten wurde. Überhaupt erschien fraglich, ob Dataport als Landesinformationsstelle eigenverantwortliche Aufgaben übertragen werden können. Der Staatsvertrag über den Beitritt des Landes Sachsen-Anhalt zur rechtsfähigen Anstalt des öffentlichen Rechts „Dataport“ lässt eine Funktionsübertragung nicht zu. Gemäß § 3 Abs. 1 Satz 1 Staatsvertrag unterstützt Dataport die öffentlichen Verwaltungen des Landes Sachsen-Anhalt. Nach § 15 Abs. 2d Staatsvertrag verarbeitet Dataport personenbezogene Daten für öffentliche Stellen in Sachsen-Anhalt. Bereits in seinem XI. Tätigkeitsbericht (Nr. 4.4) hatte der Landesbeauftragte festgestellt, dass die zuständigen Ressorts bzw. beauftragenden Behörden „verantwortliche Stelle“ gemäß § 2 Abs. 8 DSG LSA bleiben, mit der Folge, dass lediglich eine Erhebung, Verarbei-

tung oder Nutzung personenbezogener Daten im Auftrag gemäß § 8 DSG LSA erfolgen kann. In diesem Zusammenhang sieht auch die Datenschutz-Leitlinie vom 28. Mai 2014 der Fa. Dataport ausschließlich eine Verarbeitung personenbezogener Daten im „Kundenauftrag“ vor. Eine Ermächtigungsgrundlage, dass Dataport (Landesinformationsstelle) als Meldebehörde auftritt, konnte dem Staatsvertrag nicht entnommen werden. Der vorgelegte Gesetzesentwurf ging nach Auffassung des Landesbeauftragten über eine „Dienstleistung“ im Rahmen der Verarbeitung personenbezogener Daten im Auftrag hinaus, da Dataport nun als Meldebehörde auftreten soll. Der Landesbeauftragte wies zusätzlich darauf hin, dass erkennbar werden müsse, dass eine Aufgabenerweiterung nicht durch Verordnung, sondern durch Gesetz geregelt werde.

Zudem wurde deutlich, dass bei einer automatisierten Datenübermittlung Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit – entsprechend dem jeweiligen Stand der Technik – getroffen werden müssen. Diese Voraussetzungen sind regelmäßig erfüllt, wenn die eingeführte Satzbeschreibung OSCI-XMeld und das Übermittlungsprotokoll OSCI-Transport verwendet werden. Der Standard OSCI-XMeld dient der automatisierten Datenübermittlung im Meldewesen. Nach der bisherigen Rechtslage sind u. a. Datenabrufe unter Verwendung des Datenaustauschformats XMeld sowie des Übermittlungsprotokolls OSCI-Transport durchzuführen. Sofern künftig vom Landesgesetzgeber daran gedacht wird, von der Satzbeschreibung OSCI-XMeld und dem Übermittlungsprotokoll OSCI-Transport abzusehen, sind technische und organisatorische Maßnahmen zu treffen, die zu OSCI-Transport gleichwertigen Sicherheitseigenschaften (Vertraulichkeit, Integrität, Authentizität) führen.

Der Landesbeauftragte konnte bei den Empfehlungen zur Übermittlung des gebräuchlichen (Vor-)Namens an den Mitteldeutschen Rundfunk gemäß Art. 1 § 7 Abs. 1 Nr. 2 MG LSA 2015 und zu Löschungsfristen nach Art. 1 § 7 Abs. 2 MG LSA 2015 auf Veränderungen hinwirken.

Weder das Bundesmeldegesetz noch das Meldegesetz des Landes Sachsen-Anhalt verwenden die Kennzeichnung des *gebräuchlichen* (Vor-)Namens. Es ist auch nicht erkennbar, für welche Zwecke diese besondere Kennzeichnung genutzt werden soll. Gemäß § 7 Abs. 1 Nr. 2 des Entwurfes sollten alle Vornamen dem Mitteldeutschen Rundfunk übermittelt werden. Eine besondere Kennzeichnung war weder erkennbar noch erforderlich. Die Empfehlung des Landesbeauftragten, in Art. 1 § 7 Abs. 1 Nr. 2 die Worte *„unter Kennzeichnung des gebräuchlichen Namens“* zu streichen, wurde umgesetzt.

Des Weiteren sollten gemäß § 7 Abs. 2 Satz 3 erhobene Daten unverzüglich gelöscht werden, wenn feststeht, dass sie nicht mehr benötigt werden. Nicht überprüfte Daten sollten nach Satz 4 spätestens nach zwölf Monaten gelöscht werden. Unklar war, warum von der bisherigen Regelung in § 31a Abs. 2 Satz 3 MG LSA abgewichen werden sollte. Einerseits kann der Zeitraum bis zur Löschung nach § 7 Abs. 2 Satz 3 des Entwurfes so lange hinausgezögert werden, dass eine Löschung faktisch nicht erfolgt bzw. Daten länger als zwölf Monate gespeichert werden. Andererseits war nicht ersichtlich, warum „nicht überprüfte“ Daten erst nach zwölf Monaten zu löschen sind. Der Landesbeauftragte hielt entgegen, dass möglicherweise – wie nach der noch bestehenden Regelung in § 31a Abs. 2 Satz 3 MG LSA – sechs Monate ausreichen. Auch diese Empfehlung des Landesbeauftragten wurde entsprechend umgesetzt.

Mit Blick auf die Beratungen (LT-Drs. 6/3716) im Landtagsausschuss für Inneres und Sport hat der Landesbeauftragte die Gelegenheit genutzt, auf die bereits im Anhörungsverfahren des Ministeriums für Inneres und Sport mitgeteilten datenschutzrechtlichen Mängel hinzuweisen.

Kritisch sah der Landesbeauftragte auch die Regelung der Verordnungsermächtigung in Art. 1 § 9 MG LSA 2015. Durch die in § 55 Abs. 6 in Verbindung mit § 38 Abs. 5 Satz 1 BMG bestehende Länderöffnungsklausel bestünde die Möglichkeit, weitere Daten im automatisierten Abrufverfahren zur Verfügung zu stellen. Dem Landesbeauftragten ist bekannt geworden, dass der Verfassungsschutzverbund von Bund und Ländern darüber nachdenkt, die sogenannten Hausauskünfte, also Daten aller Mitbewohner eines Hauses, zu erhalten, unabhängig davon, ob sie Betroffene sind oder nicht. Über die Verordnungsermächtigung in Art. 1 § 9 Nr. 4 und 5 MG LSA 2015 wäre es grundsätzlich möglich, weitere Datenbereiche festzulegen, die nicht im Einzelnen bekannt sind, die der Gesetzgeber auch nicht kennt, die das Ministerium für Inneres und Sport dann durch das Ausfüllen dieser Regelung mittels Verordnung näher bestimmen könnte. Der Landesbeauftragte machte deutlich, dass Zweifel an der Bestimmtheit dieser Verordnungsermächtigung bestünden. Diese müsste nach Inhalt, Zweck und Ausmaß so klar sein, dass deutlich wird, welche Adressaten, welche Behörden in den Blick kommen und um welche weiteren Daten es gehen kann. Er empfahl dem Ausschuss, diese Regelung nochmals in den Blick zu nehmen und mögliche Veränderungen unter Berücksichtigung datenschutzrechtlicher Belange zu prüfen.

Der zuständige Landtagsausschuss für Inneres und Sport nahm die Hinweise des Landesbeauftragten auf, sodass nunmehr die abrufenden Stellen unter Festlegung von Anlass und Zweck weitere Daten nur abrufen dürfen, soweit diese zur Aufgabenerfüllung erforderlich sind.

Das Gesetz wurde beschlossen und am 30. Juli 2015 veröffentlicht (GVBl. LSA S. 369).

6.5.3 Aufbau und Betrieb eines Zentralen Meldedatenbestandes auf Landesebene

Im Zuge der Umsetzung des Bundesmeldegesetzes (BMG) (vgl. Nr. 6.5.1) und der Einführung des Gesetzes des Landes Sachsen-Anhalt zum Bundesmeldegesetz (BMG-AG LSA) (vgl. Nr. 6.5.2) hat das Ministerium für Inneres und Sport am Aufbau und Betrieb eines Zentralen Meldedatenbestandes auf Landesebene (ZMDB) gearbeitet.

Der ZMDB, dessen Arbeitsfähigkeit mit Inkrafttreten des BMG am 1. November 2015 gewährleistet sein musste, wird in Kooperation mit der Freien und Hansestadt Hamburg und dem Land Schleswig-Holstein in einem gemeinsamen Spiegeldatenbanksystem durch den IKT-Dienstleister der Landesverwaltung, der Anstalt des öffentlichen Rechts Dataport, realisiert und als zentrales Auskunfts- und Informationsregister für Sachsen-Anhalt betrieben.

Grundlage des ZMDB ist ein von den Meldebehörden zu liefernder Initialdatenbestand, der stichtagsbezogen an das Spiegelregister zu übermitteln und anschließend tagaktuell zu halten ist, um den jederzeitigen automatisierten Abruf nach den §§ 38

und 39 BMG durch die hierzu berechtigten öffentlichen Stellen (z. B. Polizei, Verfassungsschutz) sowie des vorausgefüllten Meldescheins durch die Zuzugsmeldebehörde nach § 23 Abs. 3 BMG sicherstellen zu können.

Dazu wurde eine Projektgruppe, der neben dem IKT-Dienstleister Dataport auch Vertreter der kommunalen Spitzenverbände, des Landesbeauftragten sowie mehrerer Meldebehörden (Pilotkommunen) angehören, gegründet. Ziel der Projektgruppe war es, die technische Anbindung der Meldebehörden, Testszenarien sowie einen Probebetrieb mit den Pilotkommunen für die Datenübermittlung aus den Melderegistern an den ZMDB vorzubereiten, um die automatisierte Kommunikation rechtzeitig vor Inkrafttreten des BMG erproben zu können. Auch die Fachverfahrenshersteller wurden mit eingebunden, damit diese für sie wichtige Informationen direkt erhalten.

Grundlage für die Datenübermittlungen ist die mit den Ländern Hamburg und Schleswig-Holstein sowie Dataport abgestimmte gemeinsame Befüllungsvorschrift, die die organisatorischen Abläufe und die technischen Voraussetzungen für eine sichere Kommunikation der Meldebehörden mit dem ZMDB verbindlich festlegt und eine Erstbefüllung des ZMDB als auch die künftige tägliche Aktualisierung des gespeicherten Datenbestands sicherstellen soll.

Eine technische und organisatorische Bewertung des ZMDB ist nur schwer möglich. Es wurde eine völlig neue Software-Installation vorgenommen. Das „alte“ Bestandssystem bleibt von diesem getrennt bestehen. Gleichwohl bestehen Überlegungen, z. B. Datenbanken aus Effizienzgründen zusammenzulegen. Eine Schutzbedarfsfeststellung soll erfolgt sein, sie liegt dem Landesbeauftragten jedoch nicht vor.

Bereits beim ersten Treffen der Projektgruppe Ende 2014 signalisierten einzelne Fachverfahrenshersteller, dass sie mit Tests beginnen wollen, jedoch aufgrund rechtlicher Erwägungen davon Abstand genommen hätten. Es bestand der Plan, die Tests mit Echtdaten durchzuführen, da es angeblich mit eigens dafür erstellten Daten nicht möglich sein soll, alle Fehler vorab zu finden. Diese Auffassung teilte der Landesbeauftragte nicht. Es wurde allen Herstellern nahegelegt, Pseudonymisierung und Anonymisierung zu nutzen, wie es auch – mangels anderslautender rechtlicher Vorschriften bzw. der Einwilligung aller Betroffenen – vom Gesetz gefordert wird. Da der erste Schritt der Funktionstest der Übertragungsinfrastruktur ist, reichten aber zu diesem Zeitpunkt noch wenige Einzeldatensätze aus. Wenn die Infrastruktur wie geplant funktioniert und somit alles sicher OSCI-verschlüsselt übertragen wird, ist zumindest die Befüllung des ZMDB sicher möglich.

Archiv-Daten sollen mit den aktuellen Daten des Melderegisters im ZMDB zu einem jeweils einheitlichen Datensatz zusammengeführt werden. Jedoch gibt es keine Ordnungsmerkmale, nach denen dies immer erfolgreich funktioniert, da Menschen neue Namen erhielten, neue Gemeindeschlüssel und Stadtteilnamen existieren, ggf. ganze Orte zusammengelegt wurden. Auch Migrationen zwischen Programmversionen oder verschiedenen Herstellern/Fachverfahren können – laut Befüllungsvorschrift nicht erlaubte – Doppeldatensätze erzeugen. Eine Lösung ist hier nur zusammen mit den Fachverfahrensherstellern zu finden. Dataport war der Meinung, dass die meisten Kommunen gar keine Archive betreiben und damit auch keine Probleme entstehen werden. Mindestens eine größere Stadt in Sachsen-Anhalt hat jedoch ein Archiv.

Kritisiert wurde vom Landesbeauftragten auch der Wunsch nach einer uneingeschränkten Eigenbestandsauskunft für Behörden. Es liegt nahe, dass jede verantwortliche Stelle „ihre“ Daten jederzeit einsehen können möchte. Warum dazu jedoch ein Vollzugriff auf alle Datensätze notwendig sein soll und nicht etwa vorgefilterte Einzeldatensätze ausreichen, ist unbekannt. Wichtiger wäre hier eine passende Aufbereitung der Daten nach Kriterien wie: Was ist neu dazugekommen; wer hat was, wann und warum geändert; oder einfache statistische Auskünfte, wie sich der Bestand entwickelt hat. Ein direkter Zugriff auf alle Daten wäre im Fall eines Sicherheitsvorfalls nur für den Hacker förderlich, der sich einfacher die komplette Datenbank kopieren könnte, ohne weitere Arbeit bezüglich der Datenabrufe investieren zu müssen.

Der Landesbeauftragte geht davon aus, dass die Hinweise und Bedenken zum Liefer- und Fachverfahren hinreichend berücksichtigt worden sind; eine Prüfung des ZMDB ist beabsichtigt.

6.5.4 Ermittlungen bei möglicher Unrichtigkeit des Melderegisters

Aus der Presse wurde dem Landesbeauftragten 2014 bekannt, dass eine Kommune in Sachsen-Anhalt ungewöhnliche Kontrollmaßnahmen vor einer Schule in einer Nachbargemeinde durchgeführt hatte. Ein Mitarbeiter der Kommune, ausgerüstet mit Fotoapparat und Headset, hatte sich vor deren Grundschule gestellt, um offensichtlich Fotos der eintreffenden Schüler und Eltern zu machen. Der durch Eltern informierte Schulleiter stellte den Mitarbeiter zur Rede und informierte die Polizei. Daraufhin hat der Mitarbeiter der Kommune die Aktion abgebrochen. Aufgrund des Abbruchs wurden keine Daten erhoben.

Die Kommune begründete die Aktion mit der Überprüfung von möglichen Unrichtigkeiten des Melderegisters. Es hätte der Verdacht bestanden, dass einzelne Elternteile und ihre grundschulpflichtigen Kinder sich nur deshalb in der Nachbargemeinde mit ihrem Wohnsitz angemeldet hätten, damit diese Kinder die dortige Grundschule besuchen könnten. Es hätte die Möglichkeit bestanden, dass sie aber real in der alten Kommune weitergewohnt hätten, es sich also um mögliche Scheinummeldungen handeln würde.

Im Vorfeld der Überprüfung vor der Schule hatte die Kommune telefonisch bei der Gemeindeverwaltung bzw. deren Grundschule personenbezogene Daten der Betroffenen abgefragt. So wurde in Erfahrung gebracht, für welche der umgemeldeten Kinder Anträge auf Hortbetreuung bzw. Schulanmeldungen vorliegen.

Die Kommune begründete ihre Recherchen sowohl vor der Schule als auch bei der Erhebung von verschiedenen personenbezogenen Daten bei der Nachbargemeinde bzw. Nachbargrundschule ausschließlich damit, dass Sie mögliche Scheinummeldungen nachweisen wollten.

Der Landesbeauftragte stellte fest, dass die Maßnahmen datenschutzrechtlich unzulässig waren. Gemäß § 2 Abs. 1 DSG LSA sind personenbezogene Daten alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Die Maßnahme vor der Schule der Nachbargemeinde stellt zumindest den Versuch einer Datenerhebung dar. Auch wenn konkret weder Bilder noch sonstige personenbezogene Daten erhoben wur-

den, stellt sie in der tatsächlich umgesetzten Form zumindest die Inaussichtstellung oder sogar eine Drohung der Datenerhebung über die dort eintreffenden Kinder bzw. deren Eltern dar.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist grundsätzlich nur zulässig, wenn entweder das DSG LSA oder eine andere Rechtsvorschrift dieses erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine Einwilligung der Betroffenen bzw. der entsprechenden Erziehungsberechtigten lag offensichtlich nicht vor.

Das Meldegesetz Sachsen-Anhalt (MG LSA), insbesondere der § 24a Abs. 3 MG LSA, auf den die Kommune allein verwiesen hat, stellt für die vorgenannten Handlungen keine Rechtsgrundlage dar. Gemäß dieser Vorschrift hat die Meldebehörde, wenn ihr zu einzelnen Einwohnern oder zu einer Vielzahl namentlich bekannter Einwohner konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit des Melderegisters vor, den Sachverhalt von Amts wegen zu ermitteln.

Selbst wenn man das Vorliegen der Voraussetzungen des § 24a Abs. 3 MG LSA im Sinne der Kommune als gegeben ansähe (Unrichtigkeit des Melderegisters), bestehen doch erhebliche Zweifel an der Rechtmäßigkeit der Maßnahme vor der Schule der Nachbargemeinde. Soweit Daten erhoben worden sind bzw. wären, sind bzw. wären diese unter dem Gesichtspunkt der nicht gegebenen Verhältnismäßigkeit rechtswidrig. Verhältnismäßig ist eine Maßnahme, wenn sie geeignet, erforderlich und angemessen ist.

Die Maßnahmen waren weder geeignet noch erforderlich, um die Richtigkeit oder Vollständigkeit des Melderegisters zu überprüfen. Vielmehr wären die Datenerhebungen vor der Schule lediglich geeignet gewesen, den Besuch einer bestimmten Schule durch bestimmte Kinder nachzuvollziehen. Zur Überprüfung mit der Zielrichtung des Nachweises eines „Scheinwohnsitzes“ hätte man die gemeldete Wohnsituation nachprüfen können bzw. müssen (Existenz der gemeldeten Adresse, Vorlage eines Mietvertrages etc.). Zumindest als Ausfluss der Auskunfts- und Mitteilungspflicht gem. § 13 MG LSA hätte die Kommune zunächst eine Anhörung der Betroffenen vornehmen müssen. Grundsätzlich wäre es auch möglich gewesen, dass das aufnehmende Einwohnermeldeamt eine Abfrage der Mietparteien beim Wohnungsgeber durchführt (§ 12 Abs. 1 MG LSA).

Das konkrete Inaussichtstellen bzw. das Drohen mit Datenerhebungen vor der Schule stellt zwar noch keine Datenerhebung dar. Jedoch ist auch hier aus dem Grundsatz der Rechtsstaatlichkeit zu fordern, dass für das beabsichtigte Verhalten der Kommune zumindest eine Rechtsgrundlage gegeben ist, die das Verhalten rechtfertigt. Dies gilt erst recht, wenn die Erhebung von Daten nur durch Zufall – hier ausschließlich aufgrund des Druckes Dritter – abgebrochen wurde.

Die Datenerhebungen zu den Schülern durch telefonische Anfragen in der Nachbarkommune bzw. bei deren Schule wurden auch ausschließlich mit dem melderechtlichen Zweck begründet und durchgeführt. Sie sind daher aus den gleichen Gründen als nicht rechtmäßig zu werten.

Im Ergebnis wurde festgestellt, dass weder das Meldegesetz Sachsen-Anhalt noch das Datenschutzgesetz Sachsen-Anhalt die angestrebten bzw. durchgeführten Datenerhebungen rechtfertigen.

Aufgrund der Tatsache, dass die Kommune ausdrücklich erklärte, dass vor der Schule keine Daten erhoben worden seien, und gleichzeitig einräumte, dass die durchgeführten Maßnahmen äußerst unglücklich gelaufen seien, geht der Landesbeauftragte davon aus, dass die Rechtswidrigkeit der Datenerhebungen in der Kommune unverzüglich erkannt wurde. Vor diesem Hintergrund und der Tatsache, dass es sich offensichtlich um einen einmaligen Einzelfall handelt, hat der Landesbeauftragte von einer ausdrücklichen Beanstandung abgesehen.

6.6 Sicherheitsakten

In seinem XI. Tätigkeitsbericht (Nr. 5.12) hat der Landesbeauftragte über die Sicherheitsakte als solche, die beschränkten Einsichts- und Auskunftsmöglichkeiten der Betroffenen und seine deshalb durchgeführten Kontrollen berichtet. Im Rahmen der Stellungnahme der Landesregierung (LT-Drs. 6/3512) wurde auf die Feststellungen des Landesbeauftragen nicht eingegangen.

Der Landesbeauftragte hat vor dem Hintergrund der bereits in der Vergangenheit geschilderten Notwendigkeit seine Kontrollen bei den Ministerien fortgesetzt. Im Berichtszeitraum wurden drei von ihnen einer Kontrolle im Hinblick auf den datenschutzgerechten Umgang mit Sicherheitsakten unterzogen. Die Ergebnisse zeigten sowohl Positives als auch Bedenkliches und bestätigten den Landesbeauftragten darin, seine Kontrollen fortzusetzen.

Bei einer Kontrolle konnte der Landesbeauftragte zwar feststellen, dass die Sicherheitsakten dem Grunde nach den gesetzlichen Vorgaben entsprechend geführt werden, dass aber seit geraumer Zeit nur ein stellvertretender Geheimschutzbeauftragter bestellt ist. Die Position des Geheimschutzbeauftragten war zum Zeitpunkt der Kontrolle wegen Pensionseintritt des ehemaligen Geheimschutzbeauftragten verwaist. Nachdem der Landesbeauftragte auf den nicht vertretbaren Umstand mit seinem Prüfbericht hingewiesen hat, wurde seitens des Ministeriums ein Geheimschutzbeauftragter bestellt.

Im zweiten überprüften Ministerium lagen keine Sicherheitsakten vor. Schneller als sonst konnte die Kontrolle deshalb aber nicht beendet werden. Zumindest für den Geheimschutzbeauftragten des Ministeriums selbst hätte eine Sicherheitsakte vorhanden sein müssen. Aus Anlass der Kontrolle wurde vorgetragen, dass diese Sicherheitsakte durch eine andere oberste Landesbehörde geführt würde. Weitere Ermittlungen ergaben allerdings, dass dies nicht der Fall war, weil die Sicherheitsakte dort bereits vernichtet wurde. Schlussendlich hätte aber das Führen einer Sicherheitsakte bei einer anderen Dienststelle ebenso gegen die Vorschriften des SÜG-LSA verstoßen, wie das Fehlen einer Sicherheitsakte. Es bedurfte dann noch eines gewissen Schriftwechsels, bis sichergestellt war, dass eine Sicherheitsüberprüfung für den Geheimschutzbeauftragten und einen Vertreter beantragt wurde.

Bei der dritten Kontrolle kam es bereits im Rahmen der Vorbereitung zu einem bemerkenswerten Umstand. Der Landesbeauftragte prüft im Voraus einer Kontrolle, ob und welche Widersprüche gegen seine Einsichtnahme in die Sicherheitsakte vorlie-

gen. Dass jedem Betroffenen ein solches Widerspruchsrecht nach § 22 Abs. 3 DSG LSA zusteht, hat der Landesbeauftragte bereits in seinem X. Tätigkeitsbericht (siehe Nr. 26.4) ausgeführt. Der Landesbeauftragte führt insoweit Übersichten zu jeder betroffenen Dienststelle, die die Personen, die Widersprüche eingelegt haben, ausweist. Die Sicherheitsakten dieser Personen schließt er dann von der Kontrolle aus. Im vorliegenden Fall lag dem Landesbeauftragten ein Widerspruch vor. Nachdem der Landesbeauftragte seine Kontrolle schriftlich angekündigt hatte, gingen bei ihm gesammelt durch den Geheimschutzbeauftragten sieben weitere Widersprüche ein. Das Auffällige daran war, dass alle diese Widersprüche so datiert waren, dass sie erst nach der schriftlichen Ankündigung der Kontrolle eingelegt wurden. Es stellte sich die Frage, warum die Betroffenen ausgerechnet zwischen Kontrollankündigung und Kontrolltermin Widerspruch erhoben hatten.

Da einer der Widersprüche lediglich in Kopie übersandt wurde, war er nicht wirksam erhoben und wäre bei der Kontrolle unbeachtlich gewesen. Weil dies aber wohl nicht im Sinne des Betroffenen gewesen wäre, hat der Landesbeauftragte mit dem Betroffenen telefonisch Kontakt aufgenommen, um darauf hinzuweisen. Aus Anlass dieses Telefonates wurde bekannt, dass der Geheimschutzbeauftragte alle sicherheitsüberprüften Personen per E-Mail von der bevorstehenden Kontrolle des Landesbeauftragten in Kenntnis gesetzt und auf die Möglichkeit des Widerspruches hingewiesen hatte. Das Gespräch mit dem Betroffenen, in dem darauf hingewiesen wurde, dass der Landesbeauftragte nicht die Betroffenen selbst, sondern vielmehr die Arbeit des Geheimschutzbeauftragten kontrolliert, endete damit, dass auf die wirksame Erhebung eines Widerspruches verzichtet wurde. Aufgrund der gewonnenen Erkenntnis hat sich der Landesbeauftragte alle E-Mails, die im Vorfeld seiner Kontrolle versandt wurden, vorlegen lassen. Denn an die Unterrichtung der Betroffenen zu ihrem Widerspruch stellt das DSG LSA bestimmte Anforderungen. Und eine Überprüfung des Wortlautes ergab, dass dieser nicht den Maßgaben der Verwaltungsvorschriften zum DSG LSA entsprach.

Anlässlich der Kontrolle und mit seinem Abschlussschreiben hat der Landesbeauftragte darauf hingewiesen, dass eine nochmalige Unterrichtung von Betroffenen, die im Zweifelsfall bereits im Rahmen des Sicherheitsüberprüfungsverfahrens auf ihr Widerspruchsrecht hingewiesen wurden, zumindest fragwürdig erscheint. Mit Blick auf die Unterstützungspflicht öffentlicher Stellen nach § 23 DSG LSA und die Aufgaben eines Geheimschutzbeauftragten nach § 5 Abs. 2 SÜG-LSA erschien dem Landesbeauftragten das Vorgehen weder mit dem einen noch mit dem anderen vereinbar zu sein. Letztendlich werden mit der Erhebung von Widersprüchen die Möglichkeiten zur Kontrolle der Rechtmäßigkeit des Handelns des Geheimschutzbeauftragten eingeschränkt. Zweck der Kontrollen des Landesbeauftragten in diesem Bereich ist die Überprüfung des Handelns des Geheimschutzbeauftragten; die Kenntnisnahme personenbezogener Daten der überprüften Personen ist nur zwangsläufige Folge.

7 Rechtspflege und Justizvollzug

7.1 Vorratsdatenspeicherung

Am 8. April 2014 hat der Europäische Gerichtshof (EuGH) die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung für unzulässig erklärt, da die Speicherung von Kommunikationsdaten ohne Verdacht auf Straftaten nicht mit EU-Recht vereinbar sei (Az.

C-293/12 und C-594/12; NJW 2014, 2169). Der Gerichtshof sieht in der Verpflichtung zur Vorratsspeicherung dieser Daten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu ihnen einen besonders schwerwiegenden Eingriff der Richtlinie in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten.

Er kommt zu dem Ergebnis, dass der Gesetzgeber beim Erlass der Richtlinie die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit einhalten müsse. Zwar sei die nach der Richtlinie vorgeschriebene Vorratsspeicherung der Daten zur Erreichung des mit ihr verfolgten Ziels geeignet, doch beinhalte sie einen Eingriff von großem Ausmaß und von besonderer Schwere in die genannten Grundrechte, ohne dass sie Bestimmungen enthalte, die gewährleisten können, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 25. April 2014 eine Entschließung verabschiedet, in der sie die Entscheidung des EuGH als wichtigen Meilenstein bei der Beachtung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses würdigt (**Anlage 12**).

Grundlage für die Umsetzung der Vorratsdatenspeicherung war die EU-Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates aus dem Jahr 2006. Die Richtlinie schrieb vor, dass Anbieter von Telekommunikationsdiensten in der EU die Verkehrsdaten ihrer Kunden mindestens sechs Monate lang speichern mussten – und zwar auch, wenn kein Tatverdacht gegen die Kunden vorlag. Gespeichert wurde, wer wann mit wem per Festnetz, Mobilfunk oder E-Mail kommuniziert hat, wer sich mit welcher IP-Adresse im Internet bewegt hat und in welchen Funkzellen sich Mobilfunknutzer aufgehalten haben. Nicht erfasst wurde dagegen der Inhalt der Kommunikation. Anlass zur Schaffung dieser EU-Richtlinie waren vor allem die Terroranschläge in Madrid 2004 und in London 2005.

Die Verfassungsgerichte Österreichs und Irlands hatten dem EuGH Klagen gegen die nationalen Regelungen zur Vorratsdatenspeicherung zur Vorabentscheidung vorgelegt. Zuvor hatten die Kärntner Landesregierung sowie insgesamt über 11.000 österreichische Bürger beim Verfassungsgerichtshof gegen die Umsetzung der Richtlinie im Land geklagt. In Irland hatte die Bürgerrechtsinitiative „Digital Rights Ireland“ gegen die Vorratsdatenspeicherung geklagt.

Der Bundestag hatte die Richtlinie bereits 2007 umgesetzt und das „Gesetz zur Neuregelung der Telekommunikationsüberwachung“ beschlossen. Ab Januar 2008 begannen Telekommunikationsunternehmen in Deutschland mit der Vorratsdatenspeicherung auf der Grundlage der neu geschaffenen §§ 113a und 113b des Telekommunikationsgesetzes (TKG). Im März 2008 schränkte das Bundesverfassungsgericht (BVerfG) nach einem Eilantrag die neuen Regelungen des TKG ein, indem es die Herausgabe der Daten nur bei schweren Straftaten und einem begründeten Anfangsverdacht erlaubte.

Am 2. März 2010 urteilte das BVerfG (NJW 2010, 833) abschließend über alle eingegangenen Verfassungsbeschwerden und erklärte das Gesetz für verfassungswidrig, da es gegen das in Art. 10 Abs. 1 GG verbriefte Post- und Fernmeldegeheimnis verstoße. Zwar sprachen sich die Richter in ihrem Urteil nicht generell gegen die Vorratsdatenspeicherung aus, mahnten jedoch erhebliche Nachbesserungen vor allem

im Hinblick auf die Verbesserung des Datenschutzes sowie mehr Transparenz und Kontrolle der Zugriffsrechte der Behörden an.

Ende Mai 2015 hat die Bundesregierung einen Gesetzentwurf vorgelegt (BR-Drs. 249/15), mit dem erneut eine Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland eingeführt werden sollte (zehn Wochen für Telefonverbindungsdaten und Internet, ohne E-Mail, und vier Wochen für Standortdaten). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aus diesem Grund am 9. Juni 2015 eine Entschließung verabschiedet, in der sie die Bundesregierung auffordert, den Gesetzentwurf in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung zu erörtern (**Anlage 30**). Wesentliche Kritikpunkte waren dabei, dass durch die Verwendung unbestimmter Rechtsbegriffe ein ausreichendes Maß an Bestimmtheit fehlt und dass der Gesetzentwurf keine Evaluierung vorsieht. Bei einem so massiven Eingriff in die Grundrechte aller Menschen unabhängig von einem konkreten Verdacht sind eine strenge Erforderlichkeits- und Verhältnismäßigkeitsprüfung vorzunehmen und die Wirksamkeit der Maßnahmen nach einer bestimmten Frist zu überprüfen.

Am 16. Oktober 2015 wurde das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom Bundestag verabschiedet (BGBl. I S. 2218). Trotz großer Bedenken von Sachverständigen erfolgte keine inhaltliche Überarbeitung der Vorschriften mehr. Allerdings wurde hinsichtlich der Überprüfung der Wirksamkeit der Maßnahmen festgelegt, dass die Bundesregierung die Vorschriften innerhalb von drei Jahren mithilfe eines externen Experten zu evaluieren hat.

Der Landesbeauftragte hat bereits in seinen früheren Tätigkeitsberichten über die EU-Richtlinie zur Vorratsdatenspeicherung, deren Umsetzung in nationales Recht und das Urteil des BVerfG berichtet (siehe VIII. Tätigkeitsbericht Nr. 23.1, IX. Tätigkeitsbericht Nr. 24.1, X. Tätigkeitsbericht Nr. 25.1 und XI. Tätigkeitsbericht Nr. 7.2) und wird auch die weiteren Diskussionen verfolgen, die u. a. durch die Terroranschläge von Paris und Kopenhagen Anfang 2015 wieder neue Nahrung erhalten haben. Allerdings muss festgestellt werden, dass auch die zwölfmonatige Vorratsdatenspeicherung in Frankreich das Attentat nicht verhindern konnte. So muss die Frage nach der Geeignetheit dieses Mittels zur Verhinderung schwerer Straftaten – insbesondere, wenn diese radikal religiös motiviert sind – auch aus datenschutzrechtlicher Sicht erneut gestellt werden (vgl. **Anlage 29**).

Die neuen Regelungen zur Vorratsdatenspeicherung werden aufgrund mehrerer Verfassungsbeschwerden vom Bundesverfassungsgericht geprüft. Dabei wird der Prüfmaßstab des EuGH (siehe Nr. 1.1) einzubeziehen sein.

7.2 Gesetz zur Weiterentwicklung des Justizvollzugs in Sachsen-Anhalt

Mit dem Gesetzentwurf zur Weiterentwicklung des Justizvollzugs in Sachsen-Anhalt vom 4. Februar 2015 (LT-Drs. 6/3799) hat der Gesetzgeber auch eine Reform des Datenschutzrechts für den Strafvollzug auf den Weg gebracht (zur korrespondierenden informationsfreiheitsrechtlichen Seite des Entwurfs vgl. den III. Tätigkeitsbericht zur Informationsfreiheit, Nr. 5.4.4). Für den Erwachsenen-, den Untersuchungshaft- und den Jugendstrafvollzug sowie für die Sicherungsverwahrung sollen prinzipiell

einheitliche datenschutzrechtliche Regelungen gelten, sofern nicht wegen der abweichenden Materie Sonderregelungen geboten sind.

Bei der Konzeption des Gesetzes hat das Ministerium für Justiz und Gleichstellung die datenschutzrechtlichen Regelungen aus dem Landesjustizvollzugsdatenschutzgesetz Rheinland-Pfalz in das neue Justizvollzugsgesetzbuch Sachsen-Anhalt (JVollzGB LSA) übernommen. Im Übrigen wurde das Datenschutzgesetz Sachsen-Anhalt für anwendbar erklärt. Es ist durchaus nicht ungewöhnlich, dass ein Landesgesetzgeber gerade bei fortschrittlichen Regelungswerken dem Vorbild anderer Bundesländer folgt. In Sachsen-Anhalt hat man allerdings übersehen, dass die Regelungen im Landesjustizvollzugsdatenschutzgesetz Rheinland-Pfalz logischerweise auf die Definitionen des rheinland-pfälzischen Datenschutzgesetzes verweisen. Diese enthalten aber vom Datenschutzgesetz Sachsen-Anhalt abweichende Begriffsbestimmungen. Die Gesetze sind also nicht miteinander kompatibel. Ein Beispiel: Sachsen-Anhalt unterscheidet traditionell zwischen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. In Rheinland-Pfalz ist die Erhebung und Nutzung personenbezogener Daten dagegen schon Teil der Datenverarbeitung. Unter dem Begriff „Datenverarbeitung“ wird in Sachsen-Anhalt und in Rheinland-Pfalz daher nicht das gleiche verstanden.

Der Landesbeauftragte hat diesen Mangel bereits im Rahmen einer ersten Anhörung durch das Ministerium gerügt und darauf hingewiesen, dass sich die datenschutzrechtlichen Regelungen grundsätzlich am Kernrecht, also am Datenschutzgesetz des Landes Sachsen-Anhalt orientieren müssen. Das Ministerium hat daraufhin versucht, zumindest die gröbsten Mängel und Ungereimtheiten, die sich durch die Übertragung fremden Landesrechts ergeben haben, im Rahmen der Überarbeitung des Gesetzesentwurfs zu beseitigen. Problematisch blieb aber nach wie vor, dass die rheinland-pfälzischen Regelungen einen Fremdkörper darstellen, der nicht zum sachsen-anhaltischen Landesrecht passt.

In der öffentlichen Anhörung vor dem Rechtsausschuss des Landtages am 19. Juni 2015 hat der Landesbeauftragte in diesem Zusammenhang darauf hingewiesen, dass der Gesetzgeber nach der Rechtsprechung bei der konzeptionellen Umsetzung seiner Regelungsvorstellungen nicht völlig frei sei. Die von ihm vorgegebenen Regelungs- und Ausnahmetatbestände müssen vielmehr einem nachvollziehbaren Konzept entstammen und dürfen weder gleichheitswidrig noch willkürlich sein. Warum nunmehr ausschließlich im Justizvollzug von den vom Gesetzgeber vorgegebenen gesetzlichen Definitionen und Regelungsstrukturen Sachsen-Anhalts abgewichen werden soll und diese durch die gesetzlichen Regelungen des Landes Rheinland-Pfalz ersetzt werden soll, hat die Landesregierung weder kenntlich gemacht noch wirklich begründet. Insbesondere fehlt es dem Gesetzentwurf der von der Rechtsprechung geforderten tiefgreifenden Begründung und Rechtfertigung, warum ein Abweichen von den bisherigen Regelungstatbeständen hier ausnahmsweise (zwingend) erforderlich ist. Die Übernahme von rheinland-pfälzischem Recht statt der Übernahme der vorhandenen datenschutzrechtlichen Regelungen aus Sachsen-Anhalt erscheint insbesondere vor der Verweisung auf die auch geltenden Regelungen des DSG LSA als willkürlich und damit verfassungsrechtlich bedenklich.

Der Landtag hat die Bedenken des Landesbeauftragten dazu im Wesentlichen aufgegriffen. Das JVollzGB LSA wurde an die Begrifflichkeiten des Datenschutzgesetzes Sachsen-Anhalt angepasst. Allerdings gibt es nun eine anwenderunfreundliche

Mischung: Neben Regelungen zur „Datenverarbeitung im Vollzug“ (§ 123 Abs. 1) finden einige Bestimmungen des DSG LSA unmittelbar Anwendung und zudem weitere Vorschriften des DSG LSA entsprechende Anwendung (§ 163). Das JVollzGB LSA ist am 1. Januar 2016 in Kraft getreten (GVBl. LSA 2015 S. 666).

7.3 PPP-Projekt Justizvollzugsanstalt Burg

Seit dem X. Tätigkeitsbericht (Nrn. 24.1 und 24.2) mahnt der Landesbeauftragte für die JVA Burg den Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung mit dem privaten Dienstleister an. Seit diesem Zeitpunkt hat das Ministerium für Justiz und Gleichstellung den Vertragsabschluss angekündigt. Zuletzt hatte das Ministerium in der Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht des Landesbeauftragten (LT-Drs. 6/3512, zu Nr. 7.3) erneut mitgeteilt, dass die erforderlichen vertraglichen Regelungen Gegenstand eines engen Abstimmungsprozesses der Parteien seien. Das war im Jahr 2014. Über ein Jahr später liegt immer noch kein Vertragswerk vor. Im Ergebnis scheint das Ministerium die Herbeiführung eines rechtskonformen Zustands nicht nachhaltig zu verfolgen.

Dagegen hat die JVA Burg auf die Kritik des Landesbeauftragten in seinem XI. Tätigkeitsbericht (Nr. 7.3) die Datenschutzdienstanweisungen für den Strafvollzug, die Untersuchungshaft und die Sicherungsverwahrung noch einmal überarbeitet. Da das Gesetz zur Weiterentwicklung des Justizvollzugs in Sachsen-Anhalt (GVBl. LSA 2015 S. 666; vgl. Nr. 7.2) auch das Datenschutzrecht für den Strafvollzug und die Sicherungsverwahrung für Sachsen-Anhalt weitgehend neu regelt, werden die Dienstanweisungen komplett überarbeitet und an die neue Rechtslage angepasst werden müssen.

7.4 Elektronischer Rechtsverkehr in der Justiz

Die Justizverwaltung des Landes steht mit der Einführung des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akte (eAkte) vor einem grundlegenden Umbruch, der auf nahezu alle Arbeitsgebiete und Beschäftigten im Justizbereich Auswirkungen haben wird.

Gemäß dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) ist der elektronische Zugang zur Justiz ab dem 1. Januar 2018 zu allen deutschen Gerichten zu ermöglichen. Das Gesetz erlaubt den Justizverwaltungen der Länder jedoch, den elektronischen Zugang bis zum 31. Dezember 2019 zu verschieben. Nach dem Gesetzeswortlaut kann diese Entscheidung jedoch nur von allen Ländern gemeinsam getroffen werden.

Sofern die Landesregierung nicht von der Möglichkeit Gebrauch macht, die Einführung des verpflichtenden ERV für Anwaltschaft und Behörden vorzuverlegen, wird seine Einführung zum 1. Januar 2022 erfolgen. Dabei müssen nicht nur die entsprechenden finanziellen Mittel eingeplant, sondern auch die Basisinfrastruktur muss dafür bereitgestellt werden. Hierzu gehören u. a. das geplante moderne, breitbandige und sichere Landesnetz ab 2018 (ITN-XT) genauso wie entsprechende verschlüsselte Basisdienste für Kommunikation und Internetnutzung, um den zukünftig erhöhten Anforderungen im Justizbereich aber auch in der übrigen Landesverwaltung zu entsprechen. Gleichzeitig muss innerhalb der Behörden des Landes hierzu Erfahrung

und Kompetenz, insbesondere zum Thema Verschlüsselung weiter ausgebaut werden (siehe Nr. 4.5).

Der Datenschutz muss insofern im Rahmen der Einführung und Umsetzung des ERV eine tragende Rolle spielen. Eine digitale Verwaltung in der Justiz und den übrigen Behörden der Landes- und Kommunalverwaltung kann nämlich nur dann funktionieren, wenn die Bürgerinnen und Bürger darauf vertrauen können, dass die elektronische Bearbeitung von Vorgängen und die elektronische Kommunikation mit der Justiz und der übrigen Verwaltung genauso sicher sind wie in der derzeitigen analogen Welt. Dem entsprechend müssen auch bei elektronisch geführten Verfahren personenbezogene Daten unversehrt, authentisch, nicht manipulierbar und vertraulich bleiben. Sie dürfen deshalb auch nicht von Unberechtigten abgefangen bzw. mitgelesen werden können. Gegenwärtig bestehen jedoch erhebliche praktische Schwierigkeiten, dies sicherzustellen. So ist z. B. das derzeitige Hauptkommunikationsmittel im Internet, nämlich die einfache*, unverschlüsselte* E-Mail, vergleichbar mit einer *Postkarte*, die von jedem lesbar ist. Sie ist unter datenschutzrechtlichen Gesichtspunkten für die Durchführung elektronischer Verfahren nicht geeignet, da der Absender nicht eindeutig bestimmbar bzw. sogar manipulierbar ist und zumindest an den Mail-Servern Kenntnisnahme und Manipulation von E-Mails durch unbefugte Dritte möglich sind.

Mit der Einführung und Nutzung des "Elektronischen Gerichts- und Verwaltungspostfaches" (EGVP) für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften des Landes Sachsen-Anhalt wird im Bereich der Justiz aus datenschutzrechtlicher Sicht der richtige Weg beschritten. Zu den wesentlichen Merkmalen des EGVP, welches damit viele datenschutzrechtliche Normen umsetzt, gehören ein “Rund um die Uhr"-Zugang zu den teilnehmenden Gerichten und Behörden mittels einer sicheren und zuverlässigen Übertragung durch Nutzung des OSCI-Standards. D. h. es erfolgt eine geschützte Kommunikation durch den Einsatz kryptografischer Mechanismen beim Signieren, Verschlüsseln und Übertragen von Nachrichten und die sofortige signierte Eingangsbestätigung durch die Empfangseinrichtung des Gerichts oder der Behörde sowie eine Unterstützung aller akkreditierten Signaturkarten nach deutschem Signaturgesetz. Die Nutzung des EGVP erfolgt auch durch eine Reihe von Behörden der Landes- und Kommunalverwaltung, ist aber noch ausbaufähig.

Die landesweite Einführung der *verschlüsselten* elektronischen Kommunikation innerhalb der Landes- und Kommunalverwaltung, mit Bürgerinnen und Bürgern und mit der Wirtschaft, sowie die Schaffung von Voraussetzungen zur Nutzung der Qualifizierten Elektronischen Signatur (QES) zur Signatur von elektronischen Dokumenten für Behörden des Landes, aber auch die datenschutzgerechte Führung von eAkten sind Themen, welche die Justiz bei der Umsetzung des ERV verstärkt beschäftigen werden. Auch hier spielt der Einsatz der QES zur Sicherstellung der Integrität elektronischer Dokumente eine wesentliche Rolle. Das eingangs genannte Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten bildet hierzu die Grundlage.

Im Rahmen einer elektronischen Aktenführung, die dann die Führung von Papierakten ersetzen soll, muss die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz der Daten gewährleistet sein (§ 6 Abs. 2 DSG LSA). Bei der Übertragung von Papierakten in die elektronische Form durch

sog. ersetzendes Scannen muss z. B. sichergestellt werden, dass ein ordnungsgemäßer Übertragungsvorgang erfolgt, da das Papierdokument anschließend vernichtet wird. Im Bereich der Justiz erfolgt hier die Pilotierung der eAkte im Finanzgericht des Landes Sachsen-Anhalt in Dessau-Roßlau.

Das Ministerium für Justiz und Gleichstellung hat zur Einführung und Umsetzung des ERV, die auch Gegenstand des IT-Ressortkonzepts 2015/2016 sind, ein Strategiegremium und einen Lenkungskreis gebildet. Das Projekt „Einführung des elektronischen Rechtsverkehrs (ERV) in der Justiz des Landes Sachsen-Anhalt“ wurde mit der 1. Sitzung des Strategiegremiums am 18. Juni 2014 eröffnet. Im Berichtszeitraum haben bisher drei Sitzungen des Lenkungskreises stattgefunden. Der Landesbeauftragte begleitet diesen Prozess der Einführung des ERV, u. a. als Mitglied dieser Gremien. Der Lenkungskreis koordiniert die Arbeit der sechs eingerichteten Arbeitsgruppen im Justizbereich, welche sich mit den Themenbereichen Gerichts-/Behördenorganisation, Akzeptanz- und Qualifikationsmanagement, Technik/Infrastruktur, Fachverfahren, Staatsanwaltschaften und Justizvollzug/Sozialer Dienst der Justiz befassen.

8 Verfassungsschutz

8.1 Reform der Sicherheitsbehörden

Zu den Reformansätzen im Bereich der Sicherheitsbehörden aufgrund der Erkenntnisse zum „Nationalsozialistischen Untergrund“ (NSU) hat der Landesbeauftragte in seinem XI. Tätigkeitsbericht (siehe Nr. 8.1) berichtet. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits im November 2012 mit ihrer Entschließung „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“ (siehe XI. Tätigkeitsbericht, Anlage 18) in die Diskussion über Reformmaßnahmen eingebracht. Auch wird auf die Grundsatzentschließungen vom 5. September 2013 (**Anlage 1**) sowie 1. und 2. Oktober 2013 (**Anlage 2**) verwiesen, die u. a. auf den NSA-Ausspähskandal reagieren.

Auf Sachsen-Anhalt bezogen waren im Berichtszeitraum nur begrenzt Reformansätze zu verzeichnen. Die neue Transparenz der Arbeit der Verfassungsschutzbehörde, die sich zunächst nur auf eine veränderte Öffentlichkeitsarbeit bezieht, ist ein schmaler Ansatz. Denn diese erfüllt nicht die Maßstäbe angemessener Informationsfreiheit (vgl. III. Tätigkeitsbericht Informationsfreiheit, Nr. 5.7.1, LT-Drs. 6/4048). Als eine strukturelle Anpassung kann die Umgestaltung bzw. Erweiterung des „Gemeinsamen Informations- und Abwehrzentrums im Landeskriminalamt Sachsen-Anhalt“ verstanden werden, über die der Landesbeauftragte unter Nr. 6.4 dieses Tätigkeitsberichtes berichtet. Änderungen der bestehenden Rechtslage mittels gesetzlicher Anpassungen zeichnen sich in Sachsen-Anhalt allerdings nicht ab. Das ist in einigen Bundesländern anders. Verschiedene Bundesländer haben mit Blick auf die Erkenntnisse um den NSU ihre Verfassungsschutzgesetze angepasst. Dabei geht es u. a. um Fragen zum Einsatz von Vertrauenspersonen („V-Leute“), Benachrichtigungspflichten gegenüber Betroffenen und die Ausgestaltung der parlamentarischen Kontrolle. Dies sind Aspekte, die auch für die Arbeit des Verfassungsschutzes im Lande Sachsen-Anhalt zu berücksichtigen sind. Deren Beantwortung lässt aber noch auf sich warten.

Auf Bundesebene hat der Deutsche Bundestag mit seinem Beschluss über das „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BT-Drs. 18/4654, 18/5051, 18/5415) verschiedene Gesetze – insbesondere das Bundesverfassungsschutzgesetz, das MAD-Gesetz, das BND-Gesetz und das Artikel 10-Gesetz – geändert und damit eingeforderte Reformen im Bereich der rechtlichen Grundlagen der Geheimdienste vorgenommen (BGBl. I 2015 S. 1938). Datenschutzrechtlich bestehen aber durchaus Bedenken gegen verschiedene der neuen Regelungen. Auf der einen Seite geht die Ausweitung der Auswerte- und Analysebefugnisse des Bundesamtes für Verfassungsschutz so weit, dass auch untergeordnete und lokal begrenzte Bestrebungen nunmehr auf Bundesebene analysiert werden dürfen. Die Art der Auswertemittel begrenzt das Gesetz auf der anderen Seite aber nicht. Für die Übermittlung von Daten der Verfassungsschutzbehörden untereinander wurde die Schwelle herabgesetzt. Wenn bisher mit Blick auf den Grundsatz der Verhältnismäßigkeit die Übermittlung zur Aufgabenerfüllung erforderlich sein musste, so reicht es nunmehr, dass die Daten relevant sind. Für den Einsatz von V-Leuten werden zwar Regelungen geschaffen, eine sachgerechte und datenschutzrechtlich zu fordernde Differenzierung des Einsatzes nachrichtendienstlicher Mittel nach der Eingriffsintensität erfolgt aber nicht. Und für die Datenübermittlung zwischen der Polizei und den Nachrichtendiensten wurden Regelungen geschaffen, die der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07; NJW 2013, 1499) widersprechen. Das Bundesverfassungsgericht hat dem Gesetzgeber für Datenübermittlungen zwischen Nachrichtendiensten und der Polizei auferlegt, nicht an niedrigschwellige Voraussetzungen wie der bloßen Erforderlichkeit zur Aufgabenerfüllung anzuknüpfen. Die Datenschutzkonferenz hat ihre Grundsatzkritik an der Verfassungsschutzreform im Herbst 2015 mit einer Entschließung bekräftigt (**Anlage 32**).

Für die Gesetzgebung auf Landesebene wird es darauf ankommen, die datenschutzrechtlich in den geschilderten Bereichen problematische Bundesgesetzgebung nicht einfach zu übernehmen. Anpassungsbedarf besteht z. B. bei § 18 des Landesverfassungsschutzgesetzes.

Mit der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“ (**Anlage 13**) fordern die Datenschutzbeauftragten den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen für der Kontrolle bisher entzogener Bereiche auszustatten, damit das vorhandene Fachwissen auch in diesem Bereich genutzt werden kann. Diese Forderung der Datenschutzbeauftragten geht auch auf die Feststellungen in den Berichten der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente, die erhebliche Kontrolldefizite auch bei den Verfassungsschutzbehörden aufzeigen, zurück. Vor dem Hintergrund der Überwachungen durch NSA und BND ist diese Thematik weiterhin hochaktuell. Im Rahmen von Gesetzgebungsverfahren auf Landesebene wird der Landesbeauftragte auf die Umsetzung der Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hinwirken.

8.2 Moratorium bei Aktenvernichtung und Löschung von Daten

In seinem XI. Tätigkeitsbericht (Nr. 8.2) hat der Landesbeauftragte über das Moratorium hinsichtlich der Vernichtung bzw. Löschung personenbezogener Daten, die im

Zusammenhang mit dem NSU stehen, berichtet. Verfassungsschutzbehörde und Polizei des Landes Sachsen-Anhalt hatten mit Blick auf die Ermittlungen des entsprechenden Bundestagsuntersuchungsausschusses vorübergehend auf die Vernichtung bzw. Löschung von insoweit relevanten Daten verzichtet.

Der Landesbeauftragte hat insbesondere darauf hingewiesen, dass der Löschung der dem Moratorium unterliegenden Daten nach Wegfall des Zwecks besondere datenschutzrechtliche Bedeutung zukomme und er das Vorgehen weiter begleiten werde. Der Bundestaguntersuchungsausschuss hat zwischenzeitlich seine Arbeit beendet (Abschlussbericht BT-Drs. 17/14600) und konkrete Anfragen aus dem parlamentarischen Raum im Land Sachsen-Anhalt zum NSU lagen nicht mehr vor.

Im Jahr 2014 wurden infolge dieses Wegfalls des Zwecks die für die Arbeit des Bundestagsuntersuchungsausschusses zunächst nicht gelöschten Daten – genau genommen die Datenträger, auf denen sie gespeichert waren – beim Landeskriminalamt und bei der Verfassungsschutzbehörde vernichtet. Der Landesbeauftragte hat sich die entsprechenden Vernichtungsnachweise vorlegen lassen.

8.3 Kontrolle der Antiterrordatei

In seinem XI. Tätigkeitsbericht hat der Landesbeauftragte zum Thema „Anti-Terror-Maßnahmen“ (Nr. 5.3) ausgeführt und in diesem Zusammenhang auch die Antiterrordatei als Verbunddatei beschrieben und die Entscheidung des Bundesverfassungsgerichtes zum Antiterrordateigesetz vom 24. April 2013 (1 BvR 1215/07; NJW 2013, 1499) erläutert. Insbesondere das vom Bundesverfassungsgericht beschriebene informationelle Trennungsprinzip beim Datenaustausch zwischen Polizei und Verfassungsschutz ist als Anforderung aus dem Grundrecht auf informationelle Selbstbestimmung von grundlegender Bedeutung.

Neben den Erwägungen zur Verfassungsmäßigkeit der Regelungen im Antiterrordateigesetz hat das Bundesverfassungsgericht u. a. ausgeführt, dass angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz der regelmäßigen Durchführung von Kontrollen besondere Bedeutung zukommt. Diese Kontrollen sind in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat insbesondere den Aspekt der Kontrolle zum Anlass genommen, mit einer Entschließung vom 8. und 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“ (**Anlage 13**) auf die Erfordernisse hinzuweisen. Wie das Bundesverfassungsgericht hat die Konferenz verdeutlicht, dass diese Anforderungen an effektive Kontrolle bei der Ausstattung der Datenschutzbeauftragten in Bund und Ländern zu berücksichtigen sind.

Aufgrund der Entscheidung des Bundesverfassungsgerichtes wurde das Antiterrordateigesetz durch das „Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze“ vom 18. Dezember 2014 (BGBl. I 2014 S. 2318) geändert. Die Änderungen traten zum 1. Januar 2015 in Kraft. Mit § 10 Abs. 2 ATDG wurden die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesbeauftragten für Datenschutz im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes beim Betrieb der Antiterrordatei zu kontrollieren.

Der Landesbeauftragte hatte sich mit den Speicherungen in der Antiterrordatei bereits nach ihrer Errichtung im Jahr 2007 befasst und auf vorzunehmende Änderungen hingewirkt. Vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichtes und der nunmehr nach § 10 Abs. 2 ATDG bestehenden Rechtslage hat der Landesbeauftragte 2015 erneut eine Kontrolle zu den Speicherungen in der Antiterrordatei, der Nutzung der Antiterrordatei und der technischen und organisatorischen Absicherung bei der Verfassungsschutzbehörde und beim Landeskriminalamt durchgeführt. Datenschutzrechtliche Verstöße musste der Landesbeauftragte dabei nicht feststellen.

8.4 Ausstiegsprogramm des Verfassungsschutzes

Der Landtag von Sachsen-Anhalt beschäftigt sich seit einigen Jahren mit Fragen der Entwicklung des Rechtsextremismus in Sachsen-Anhalt und mit Gegenmaßnahmen der Landesregierung. Einen Aspekt dieser Befassung bildete auch die Neuausrichtung von Ausstiegsprogrammen. Die grundsätzliche Frage, wer Ausstiegshilfe sinnvoll und erfolgversprechend anbieten kann, nahm bei den Befassungen insbesondere im Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt einen umfassenden Raum ein. Letztendlich war es das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, das durch seine Abteilung 4 – die Verfassungsschutzbehörde – ein entsprechendes Programm erarbeiten und umsetzen sollte.

Unabhängig von den Informationen zu Ausstiegsprogrammen im Rahmen der parlamentarischen Diskussion hat sich der Landesbeauftragte im März 2013 erstmalig mit einer Feinkonzeption zur „Neukonzeption der Ausstiegshilfe Rechts Sachsen-Anhalt“ durch das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt befasst. Aufgrund der parallel im Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt geführten Erörterungen und einer entsprechenden Anhörung hat sich der Landesbeauftragte zunächst gegenüber dem Ausschuss geäußert und u. a. festgestellt, dass datenschutzrechtliche Aspekte im vorliegenden Feinkonzept nicht aufgegriffen werden.

Im März 2014 wandte sich das Ministerium für Inneres und Sport mit einem Erlassentwurf zur Einrichtung des „Kooperativen Modellprojektes ‚Extremismus-Ausstieg‘ (EXTRA)“ an den Landesbeauftragten. In Beratungen zwischen dem Ministerium für Inneres und Sport und dem Landesbeauftragten wurden grundlegende Fragen zu den Rechtsgrundlagen, der Struktur und Organisation von EXTRA, der Einhaltung des Trennungsgebotes und der Einwilligungserklärung der Betroffenen erörtert. Neben Fragen zu den rechtlichen Grundlagen hat der Landesbeauftragte besonderes Augenmerk auf die Einhaltung des Trennungsgebotes gelegt.

Kernfrage in diesem Zusammenhang ist, wie die Trennung zwischen Polizei und Verfassungsschutz gewährleistet werden kann, wenn die Verfassungsschutzbehörde die Ausstiegshilfe koordiniert, und dabei intervenierend operativ tätig wird und sich der Mitarbeit von Sozialarbeitern bedient, die bei der Polizei beschäftigt sind. Die Einhaltung des Trennungsgebotes durch verschiedene organisatorische Sicherungsmaßnahmen wurde wiederholt diskutiert, ein Konsens konnte hier aber letztendlich – wie auch bei Fragen der rechtlichen Grundlagen – nicht erzielt werden.

Mitte August 2014 wurde der Landesbeauftragte durch das Ministerium für Inneres und Sport darüber informiert, dass das „Kooperative Modellprojekt ‚Extremismus-

Ausstieg‘ (EXTRA)“ im Juli seine Arbeit aufgenommen hat. Allerdings erfolgte diese Information zeitlich erst nach der Bekanntgabe des Starts des Ausstiegsprogramms EXTRA durch Pressemitteilung Nr. 34/2014 des Ministeriums für Inneres und Sport vom 5. August 2014.

Der Landesbeauftragte hat sich Ende 2014 darüber unterrichten lassen, wie EXTRA angenommen wird und wird ggf. im Rahmen von Kontrollen weiter auf die Einhaltung datenschutzrechtlicher Anforderungen hinwirken.

9 Forschung, Hochschulen und Schulen

9.1 Forschung

9.1.1 Allgemeines

Im Berichtszeitraum wurde der Landesbeauftragte bei 19 neuen Forschungsprojekten beteiligt. Hierbei handelte es sich hauptsächlich um medizinische Studien, aber auch um Projekte aus den Bereichen Natur, Energie, Polizei und Justiz. Außerdem waren erneut durch im Berichtszeitraum stattfindende Erhebungswellen der großen Bildungsstudien, wie das Nationale Bildungspanel (NEPS), das Programme for International Student Assessment (PISA) und der IQB-Ländervergleich, entsprechende Datenschutzkonzepte, Einverständniserklärungen und Fragebögen zu prüfen. Darüber hinaus hat der Landesbeauftragte die Langzeit-Bevölkerungsstudie Nationale Kohorte begleitet (siehe Nr. 9.1.3).

9.1.2 TMF-Leitfaden

Aufgrund der zunehmenden Vernetzung medizinischer Forschung und dem damit einhergehenden Bedarf an zentralen Datenbanken, Registern und Biobanken hat die Technologie- und Methodenplattform für die vernetzte Forschung e. V. (TMF) bereits 2003 einen „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten“ verfasst und mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt. Damit lagen verschiedene Modelllösungen vor, die zum einen die Persönlichkeitsrechte der Patienten wahrten und zum anderen die für die Forschung relevanten Datensätze verfügbar machten. Im Jahr 2013 wurde der Leitfaden von der TMF überarbeitet und im Rahmen des Arbeitskreises Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder ausführlich beraten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bei ihrer Sitzung im März 2014 beschlossen, medizinischen Forschungseinrichtungen und -verbünden die neuen generischen Datenschutzkonzepte der TMF als Basis für die konkrete Ausgestaltung von Datenschutzkonzepten zu empfehlen. Das Gesamtkonzept enthält nunmehr vier Module (Klinisches Modul, Studienmodul, Forschungsmodul, Biobankenmodul), die je nach Zielrichtung des einzelnen Forschungsverbundes einzeln oder auch kombiniert verwendet werden können. Es beschreibt, wie Forschungsverbünde datenschutzgerecht aufgebaut und betrieben werden können, und erläutert, wie Datenschutzanforderungen umgesetzt werden können (z. B. Patientenaufklärung und -einwilligung, Anonymisierung, Pseudonymisierung, informationelle Gewaltenteilung, Datentreuhänder, technisch organisatorische Maßnahmen).

9.1.3 Nationale Kohorte

Wie bereits im XI. Tätigkeitsbericht (Nr. 9.1.2) dargestellt, sind auch Einrichtungen aus Sachsen-Anhalt an dem großen, bundesweiten Forschungsprojekt „Nationale Kohorte“ beteiligt. Ein Studienzentrum befindet sich in der Medizinischen Fakultät der Martin-Luther-Universität Halle-Wittenberg. Darüber hinaus hat der Nationale Kohorte e. V. festgelegt, dass die Erfassung von Sekundär- und Registerdaten deutschlandweit u. a. durch das Institut für Sozialmedizin und Gesundheitsökonomie der Otto-von-Guericke-Universität Magdeburg erfolgt. Die datenschutzrechtlichen Aufsichtszuständigkeiten verteilen sich für das Datenschutzkonzept des Vereins auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und für die Umsetzung in den lokalen Einrichtungen auf die jeweils zuständigen Landesbeauftragten.

Erste von der Martin-Luther-Universität Halle-Wittenberg eingereichte Unterlagen wurden aus datenschutzrechtlicher Sicht geprüft. Hinsichtlich der technischen und organisatorischen Maßnahmen ergaben sich einige Fragen (z. B. zur Speicherung von Zutritten und Zutrittsversuchen zum Serverraum, Passwörtervergabe, Bildschirmsperren), die sich jedoch klären ließen.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hatte zum ersten Datenschutzkonzept der Nationale Kohorte e. V. Stellung genommen. Dabei wurde angemerkt, dass ein IT-Sicherheitskonzept noch nicht zu allen Einrichtungen vorliege, die Einwilligungserklärungen nicht transparent und die Zeitpunkte der Datenlöschung nicht geregelt seien, die Nutzung der Daten um kommerzielle Zwecke erweitert würde und das Pseudonymisierungsverfahren sowie die Herausgabe an Dritte nicht hinreichend konkret dargestellt würden. Im Herbst 2014 fand der offizielle Start des Projektes statt. Zwischenzeitlich liegt auch ein sehr differenziertes, von der Bundesbeauftragten grundsätzlich positiv bewertetes Datenschutzkonzept vor. Es bedarf in einzelnen Aspekten noch der Ergänzung und Bewertung. Der Landesbeauftragte plant, sowohl beim Studienzentrum in Halle als auch beim Kompetenzzentrum Sekundärdaten Beratungs- und Informationsbesuche vor Ort durchzuführen, um auch in der konkreten Umsetzung der Konzeptionen auf datenschutzgerechtes Vorgehen hinzuwirken.

9.1.4 Gesundheitsdaten aus DDR-Zeiten

Im Berichtszeitraum erreichte den Landesbeauftragten ein Konzept eines Forschungsprojektes, das vorsah, Probanden aus einer Forschungsarbeit an Schülern in der DDR zu recherchieren und neu zu untersuchen. Diese Forschungsarbeit soll eine offizielle Studie eines DDR-Institutes gewesen sein. Ein damals beteiligter Forscher hätte die Daten aufgrund der Auflösung des Institutes bis heute privat verwahrt und würde diese nunmehr zu weiteren Forschungszwecken zur Verfügung stellen. Bei den Daten würde es sich um medizinische Daten von ca. 1800 Kindern und Jugendlichen handeln, die innerhalb der Schuluntersuchungen zusätzlich und mit Einverständnis der Eltern in den Jahren ab 1977 befragt und untersucht worden seien. Unterlagen oder auch Informationen zur organisatorischen Einbindung des damaligen Projektes bzw. zu Einwilligungsinhalten wurden dem Landesbeauftragten nicht vorgelegt. Eine präzise und abschließende Bewertung war damit nicht möglich.

Zunächst war unklar, ob die im Rahmen der DDR-Studie erhobenen Daten auch der ärztlichen Schweigepflicht unterliegen. Darüber hinaus war aus den Unterlagen nicht zweifelsfrei festzustellen, welche Stelle damals als datenschutzrechtlich verantwortliche Stelle gehandelt hat. Einerseits wurden die Daten wohl im Rahmen der Schuluntersuchungen durch Mitarbeiter des Gesundheitswesens eines DDR-Kreises erhoben, sodass die Daten daher zunächst der seinerzeitigen Kreisverwaltung zugestanden haben könnten und somit ggf. einer heutigen Landkreisverwaltung zustehen. Denn § 33 Abs. 1 DSG LSA regelt, dass personenbezogene Daten aus DDR-Einrichtungen demjenigen Träger öffentlicher Verwaltung zustehen, der für die Verwaltungsaufgabe zuständig ist. Angesichts des Alters der Daten und der üblicherweise gebotenen Löschung medizinischer Daten nach zehn Jahren könnte die aktuelle Speicherung allerdings unzulässig sein. Wären die Daten bei einer öffentlichen Stelle vorhanden und noch zulässig gespeichert, könnte § 27 DSG LSA in Betracht gezogen werden. Die Vorschrift regelt die Verwendung von Daten, die für Forschungszwecke erhoben sind. Es müsste sich dann um Datenbestände handeln, die deutlich jenseits der schulrechtlichen Gesundheitsüberwachungsaufgabe liegen. Andererseits könnten die Daten aber auch dem ehemals tätigen medizinischen Institut zustehen. Bei dessen Fortbestehen wäre weiter zu prüfen, ob das Institut öffentlich-rechtlicher oder privater Natur ist und damit eine Nutzung der Daten zur Kontaktaufnahme ggf. über § 27 DSG LSA oder nach § 40 BDSG möglich wäre. Die Daten dürfen dann infolge der Zweckbindung grundsätzlich nur für Forschungsprojekte verwendet werden.

9.2 Datenschutz in Schulen

Auch in diesem Berichtszeitraum hat der Landesbeauftragte mehrere Schulen hinsichtlich der Einhaltung der datenschutzrechtlichen Vorschriften anlassunabhängig geprüft. In allen kontrollierten Schulen musste festgestellt werden, dass keine behördlichen Datenschutzbeauftragten nach § 14a DSG LSA bestellt waren, obwohl automatisierte Datenverarbeitungsverfahren verwendet werden (siehe auch Nr. 9.2.1). Darüber hinaus hat der Landesbeauftragte fehlende Einwilligungserklärungen bei Datenübermittlungen von personenbezogenen Schülerdaten mittels Aushang oder Veröffentlichung auf der Homepage und fehlende schriftliche Genehmigungen der Schulleitungen bei der Verarbeitung personenbezogener Schülerdaten auf privaten Lehrerrechnern festgestellt. Mit datenschutzrechtlichen Empfehlungen wurde auf Änderungen hingewirkt.

9.2.1 Behördliche Datenschutzbeauftragte in Schulen

Wie bereits im XI. Tätigkeitsbericht (Nr. 9.3.1) dargestellt, musste der Landesbeauftragte einen erheblichen Mangel bei der Einsetzung von behördlichen Datenschutzbeauftragten in Schulen feststellen. Auch alle in diesem Berichtszeitraum kontrollierten Schulen hatten bis dahin keinen behördlichen Datenschutzbeauftragten bestellt. Das Kultusministerium des Landes Sachsen-Anhalt beabsichtigte, das Problem mittels eines Erlasses näher zu regeln. Der Erlassentwurf lag dem Landesbeauftragten zur Prüfung vor. Seine Hinweise fanden Berücksichtigung (z. B. hinsichtlich der Hervorhebung der gesetzlichen Verpflichtung der Bestellung und einer klaren Formulierung zur Vermeidung von Interessenkonflikten). Weshalb sich die seit Jahren angemahnte Erfüllung der gesetzlichen Verpflichtungen so lange hinzieht – der Erlass war im Übrigen Ende 2014 abschließend abgestimmt, aber auch Ende 2015 noch

nicht veröffentlicht –, ist dem Landesbeauftragten nicht bekannt. Er wird nach Inkrafttreten des Erlasses dessen Einhaltung kontrollieren.

9.2.2 Nutzung sozialer Netzwerke in Schulen

Im Berichtszeitraum wurde der Landesbeauftragte darauf aufmerksam, dass auch Schulen Fanpages auf Facebook betreiben und dienstlich über Facebook kommunizieren. Da der Landesbeauftragte die Auffassung vertritt, dass Schulen darauf verzichten sollten (siehe oben, Nr. 5.8.1), hat er das Kultusministerium des Landes Sachsen-Anhalt um Mitteilung gebeten, ob und welche Regelungen diesbezüglich in Sachsen-Anhalt existieren. Das Kultusministerium teilte daraufhin mit, dass die Auffassung des Landesbeauftragten vollumfänglich geteilt werde. Eine Handreichung sei jedoch nicht geplant, da die Lehrer verantwortungsbewusst damit umzugehen wüssten. Der Landesbeauftragte hielt es demgegenüber für dringend geboten, eine Orientierung oder Handreichung für die Schulen zu veröffentlichen. Themen wie das Verbot von Zwangsmitgliedschaften, Distanz zwischen Dienst- und Privatsphäre bei Lehrern und Datensicherheit (§ 6 DSG LSA) seien zu beachten. Dabei sei auch zu bedenken, dass Geheimdienste auf personenbezogene Nutzerdaten von sozialen Netzwerken zugreifen. In vielen anderen Bundesländern wurden daher entsprechende ministerielle Vorgaben verfasst. Das Kultusministerium schloss sich letztlich an und veröffentlichte Hinweise zum Thema im Schulverwaltungsblatt des Landes Sachsen-Anhalt (19. November 2014, 1/2015, S. 8). In den schmalen „Hinweisen zum Umgang mit sozialen Netzwerken“ wird erläutert, dass soziale Netzwerke im Rahmen des Erwerbs von Medienkompetenz in Unterrichtseinheiten zu Demonstrationszwecken genutzt werden können, wenn niemand zur Anmeldung gezwungen wird. Zur Übermittlung dienstlicher oder personenbezogener Informationen dürfen soziale Netzwerke nicht genutzt werden.

9.2.3 Lernplattformen

Immer mehr Schulen nutzen online-Lernplattformen für Unterrichtszwecke. Über die eingerichteten Benutzerkonten können z. B. Arbeitsblätter, Lernmaterialien oder (Haus-)Aufgaben eingestellt, bearbeitet und kontrolliert werden. Der Zugriff erfolgt von Lehrern, Schülern und ggf. auch Eltern mit einem Endgerät über das Internet in der Schule oder von zu Hause aus. Damit wird eine Vielzahl von Schüler- und Lehrerdaten webbasiert verarbeitet.

Die Arbeitsgruppe Datenschutz und Schule der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet derzeit die „Orientierungshilfe für Online-Lernplattformen im Schulunterricht“, die Mindestkriterien für Online-Lernplattformen beschreibt. Darüber hinaus hat der Landesbeauftragte den Verweis auf *Moodle* in den „Hinweisen zum Umgang mit sozialen Netzwerken“ (Bekanntmachung des Kultusministeriums des Landes Sachsen-Anhalt vom 19. November 2014, siehe Nr. 9.2.2) zum Anlass genommen, das aktuelle Datenschutzkonzept zu prüfen und einige datenschutzrechtliche Hinweise zu geben. Bei Moodle handelt es sich um eine kostenfreie Lernplattform, die in Sachsen-Anhalt auf dem Bildungsserver vom Landesinstitut für Schulqualität und Lehrerbildung Sachsen-Anhalt (LISA) technisch betreut wird. Fraglich war zunächst die Verbindlichkeit der Teilnahme der Schüler und Lehrer, wenn sich eine Schule entscheidet, Moodle als digitales Lehr- und Lernangebot zu verwenden. Bisher wurde den Eltern bzw. Schülern eine „Datenschutzer-

klärung zur schulischen Nutzung der Lernplattform Moodle“ vorgelegt und um das Einverständnis der Datenspeicherung gebeten. Im Interesse der Transparenz ist die Vorlage der Datenschutzerklärung zu begrüßen. Allerdings ist die Einholung einer Einwilligung als Rechtsgrundlage der Datenverarbeitung dann nicht erforderlich und könnte sogar bei Nichterteilung der Einwilligung problematisch werden, wenn die verbindliche Teilnahme vorgesehen ist. Soweit die Nutzung des Systems der Erfüllung der schulischen Bildungsaufgaben dient und insoweit erforderlich ist, ist die Rechtsgrundlage der Datenverarbeitung in § 84a SchulG LSA gegeben. Lediglich für nicht verbindliche Datenverarbeitungen bedürfte es einer Einwilligung als Rechtsgrundlage (§ 4 Abs. 2 DSG LSA). Wegen der unterschiedlichen Rechtsgrundlagen und Verbindlichkeit müsste für die jeweilige Verarbeitung klar erkennbar sein, worum es sich handelt.

Nach Mitteilung des Kultusministeriums handelt es sich zunächst um ein freiwilliges Lernangebot, sodass die Teilnahme eine Einwilligungserklärung erforderlich macht. Der Teil der Datenschutzerklärung, der von einer verbindlichen Teilnahme spricht, wurde daher gestrichen. Sofern durch einen Beschluss der Gesamtkonferenz der Schule die verbindliche Nutzung der Lernplattform festgelegt wurde, klärt nun ein Informationsschreiben auf, deren Kenntnis die Eltern mit Unterschrift bestätigen. Darüber hinaus erfolgt der Aufruf von Moodle auf dem Landesbildungsserver unverschlüsselt. Die unverschlüsselte Kommunikation von pflichtigen schulischen Inhalten und Zugangs- bzw. Anmeldungsdaten ist datenschutzrechtlich nicht hinnehmbar und entspricht nicht den Vorgaben des § 6 DSG LSA. Eine entsprechende Umstellung soll nach Mitteilung Kultusministeriums des Landes Sachsen-Anhalt zeitnah erfolgen.

Weitergehender Regelungsbedarf besteht allgemein im Hinblick auf die technische und organisatorische Ausgestaltung und auf die Verwendung von gespeicherten Inhalts- und Verbindungsdaten. Dies betrifft auch den passwortgeschützten Zugang zum System. Soweit der Zugriff innerhalb einer Schule über WLAN erfolgt, ist zudem der dadurch entstehenden Gefahr des Zugangs Unbefugter durch entsprechende Maßnahmen zu begegnen. Die allgemeine Erstellung von Profilen ist zu vermeiden.

9.2.4 Informationsaustausch zwischen Schule und Ausbildungsbetrieb

Zwei Auszubildende wandten sich mit der Bitte um Unterstützung an den Landesbeauftragten. Ihre berufsbildende Schule hatte auf einem Vordruck Bewertungen (sehr gut, gut, weniger gut, schlecht) in den Bereichen Betragen, Mitarbeit, Lernverhalten und Sozialverhalten ausgefüllt und dem Ausbildungsbetrieb zur Verfügung gestellt. Die Bewertungen der beiden Auszubildenden waren teilweise weniger gut bzw. schlecht. Sie erhielten umgehend die Kündigung zum Ablauf der vier Tage später endenden Probezeit.

Nach ausführlichem Schriftwechsel mit der berufsbildenden Schule, dem Kultusministerium des Landes Sachsen-Anhalt sowie Nachfragen bei einer Industrie- und Handelskammer und weiteren berufsbildenden Schulen stellte sich der Sachverhalt und die datenschutzrechtliche Bewertung wie folgt dar: Die Berufsschule bot Veranstaltungen zum Austausch über aktuelle Entwicklungen an. Eine Bildungsgesellschaft als Vertreterin mehrerer Ausbildungsbetriebe nahm regelmäßig daran teil. Während dieser Termine würden auch Fehlleistungen von Auszubildenden erörtert, um deren Situation zu verbessern. Das Angebot der Berufsschule, den Unternehmen

Leistungseinschätzungen zu übermitteln, habe die Bildungsgesellschaft angenommen und einen entsprechenden Vordruck zur Verfügung gestellt.

§ 1 der Anlage 1 zu § 36 der Verordnung über berufsbildende Schulen (BbS-VO) in der seinerzeit gültigen Fassung sah vor, dass Berufsschulen mit den anderen an der Berufsausbildung Beteiligten zusammenarbeiten. Dies ist jedoch eine reine Aufgabenbeschreibung und keine Übermittlungsbefugnis für personenbezogene Daten. Als Rechtsgrundlage kam daher § 84a Abs. 8 SchulG LSA in Betracht. Dieser setzte die Erforderlichkeit voraus, d. h. die Unerlässlichkeit der Datenverarbeitung für eine konkrete Aufgabenerfüllung. Die Notwendigkeit zur Aufgabenerfüllung muss dabei im angemessenen Verhältnis zur Beeinträchtigung des Persönlichkeitsrechts des Betroffenen stehen. Hier liegt nahe, dass kritische Bewertungen unmittelbar vor Ablauf der Probezeit dazu genutzt werden können, ein (weiterer) Anlass zur Beendigung des Ausbildungsverhältnisses mit all seinen negativen Folgen für die Betroffenen zu sein. Ausgehend davon, dass die entlassenen Auszubildenden nach knapp drei Monaten des Ausbildungsjahres für das Jahr kaum eine neue Ausbildungsstelle finden dürften, sind die Folgen erheblich.

Die konkrete Erforderlichkeit hinsichtlich der erfolgten Datenübermittlungen war trotz Nachfrage nicht zu erkennen. Es wurde seitens der berufsbildenden Schule lediglich pauschal auf „übliche“ Anforderungen und einen Leistungsbewertungserlass hingewiesen. Der Erlass zur Leistungsbewertung und Beurteilung an berufsbildenden Schulen (RdErl. des Kultusministeriums vom 1. Dezember 2010 – 31-83202) legt zu Leistungserhebungen grundsätzlich in Nr. 1.3 fest, dass sie jeweils eine angemessene Unterrichtszeit voraussetzen. Wie von der berufsbildenden Schule mitgeteilt, fanden bis zur Bewertung nur 24 Berufsschultage statt. Es war nicht ersichtlich, ob in dem kurzen Zeitraum überhaupt sachgerechte und belastbare Beurteilungen zu Merkmalen erstellt werden können, die einen sehr weiten Einschätzungs- und Fehlbeurteilungsspielraum eröffnen. Die vier Benotungsstufen des Vordrucks stimmten nicht mit den Vorgaben des § 6 BbS-VO (sechs Notenstufen) überein. Auch fanden sich keine entsprechenden Vorgaben im o. g. Erlass in Bezug auf die bewerteten Leistungsbereiche Betragen, Mitarbeit, Lernverhalten und Sozialverhalten. Es lag daher keine nachvollziehbare Begründung dafür vor, weshalb auf bloße Vorlage des Vordrucks gesondert zu den dortigen vier Merkmalen mit nur vier Benotungsstufen zu diesem Termin Äußerungen zur Sicherung einer erfolgreichen Berufsausbildung unerlässlich waren. Eine Abwägung der Gefahren für die betroffenen Schülerinnen und Schüler mit der Bedeutung, die die Informationen für die Ausbildung und den Ausbildungsbetrieb haben, war nicht dargelegt. Es gab keine Hinweise dazu, weshalb die übermittelten Bewertungsinformationen für den kündigenden Ausbildungsbetrieb erforderlich waren. Lediglich die Erläuterung der Bildungsgesellschaft wies allgemein darauf hin, dass die Zeugnisse des 1. Halbjahres für die Einschätzung der Probezeit zu spät kämen. Es konnte daher nicht einmal vermutet werden, dass es für eine sachgerechte und differenziert abgewogene Entscheidung des Ausbildungsbetriebs zur Abrundung noch ergänzender Informationen zum schulischen Lern- und Sozialverhalten bedurfte. Insgesamt bestanden daher, nach dem erreichbaren Ermittlungsstand, erhebliche Bedenken gegen die datenschutzrechtliche Zulässigkeit der Übermittlung derartiger Bewertungsbögen zu Auszubildenden.

Der Landesbeauftragte wandte sich daher an das Kultusministerium und wies auf die unklare Rechtslage und die nicht unerheblichen Gefahren hin. Auch in den angefragten weiteren Stellen (Industrie- und Handelskammer, Berufsbildende Schulen) be-

stand keine hinreichende Vorstellung über den Umfang eines zulässigen Datenaustauschs. Vielmehr wurde auf „übliche Anforderungen einer Berufsausbildung“ oder darauf hingewiesen, dass das Zusammenwirken beider Lernorte eben einen Austausch erfordere. Deshalb hatte der Landesbeauftragte seine Mithilfe angeboten und vorgeschlagen, für den zulässigen Austausch zwischen berufsbildenden Schulen und Ausbildungsbetrieben Vorgaben zu formulieren, um zumindest eine gewisse Orientierung und auch Sicherheit für die Lehrkräfte zu erreichen. Dazu sollten die Praktiker der berufsbildenden Schulen und der Ausbildungsbetriebe bzw. vertretende Organisationen einbezogen werden. Auf Möglichkeiten, in den rechtlichen Vorgaben Grenzen des Datenaustauschs darzustellen, die ein sachdienliches Zusammenwirken ermöglichen, aber Ausuferungen vermeiden, wurde hingewiesen. Leider hat das Kultusministerium die Anregung nicht aufgegriffen und stattdessen in einer novellierten BbS-VO vorgesehen, dass sich Berufsschule und Ausbildungsbetrieb zur Sicherung einer erfolgreichen Berufsausbildung gegenseitig über den Leistungsstand und das Lern- und Sozialverhalten der Auszubildenden informieren können. Dies ist leider eine Verschlechterung zu Lasten der Schülerinnen und Schüler, da sich die Ausbildungspartner nun wohl stets und noch pauschaler für jeglichen Datenaustausch auf die Rechtsgrundlage der BbS-VO berufen werden. Nähere Vorgaben zur Zulässigkeit und Erforderlichkeit einzelner Datenübermittlungen bleiben offen. Es steht zu befürchten, dass die Zahl der Schülerinnen und Schüler steigt, die Opfer einer unzulässigen Datenübermittlung mit ggf. schwerwiegenden Folgen für die berufliche Entwicklung werden.

9.3 Änderung des Schulgesetzes – gläserner Schüler

Im XI. Tätigkeitsbericht (Nr. 9.4) hatte der Landesbeauftragte über die Novellierung des Schulgesetzes berichtet, das im Dezember 2012 in Kraft trat (GVBl. LSA S. 560). Grundlegende Bedenken blieben bestehen, wie z. B. hinsichtlich einer statistischen Totalerfassung, sowie Zweifel an der Notwendigkeit einer zentralen Verwaltungsdatei, an der Notwendigkeit einer landeseinheitlichen Schülernummer und an der Anonymität des Kerndatensatzes. Zu der zentralen Schülerdatei für Verwaltungsaufgaben (§ 84c) und zur Datei für Schülerlaufbahnstatistiken (§ 84d) sollten Rechtsverordnungen folgen, die das Nähere regeln. Bis August 2015 lagen dem Landesbeauftragten noch keine erörterungsfähigen Entwürfe oder Fragestellungen vor. Das Kultusministerium stellte damit die Sinnhaftigkeit der Regelungen selbst in Frage. Erst im September 2015 ging ein umfassender Entwurf einer Rechtsverordnung ein, deren Prüfung infolge des Vorgangs Bildungspartnerschaft des Landes mit Microsoft (siehe Nr. 1.4) zunächst zurückgestellt werden musste.

Die Umsetzung der Vorhaben bedarf der Unterstützung durch Hardware und Schulverwaltungssoftware. Hierzu plant das Ministerium die Anschaffung einer Schulorganisationssoftware mit schulischen und zentralen Komponenten. In einem ersten Gespräch wurde der Landesbeauftragte über den Planungsbeginn und -stand informiert. Der Landesbeauftragte erläuterte dazu die Notwendigkeit detaillierter Betrachtung einzelner Geschäftsprozesse und der darin einbezogenen Daten sowie der daran beteiligten Personen. Wichtig sei weiterhin die Trennung von Datenbeständen für Verwaltungszwecke und für statistische Zwecke. Im letzteren Fall sollten die Datenlieferungen direkt an die für die Erstellung der Statistiken zuständige Stelle transferiert werden. Ein weiterer wesentlicher Punkt sei die frühzeitige Berücksichtigung von Löschungsroutinen. Seitens des Landesbeauftragten wurde weiter betont, dass ver-

mieden werden muss, sowohl die Verwaltungsdaten als auch die statistischen Daten in einer Stelle anfallen zu lassen.

10 Archivwesen

10.1 Novellierung des Archivrechts

Der Schutz personenbezogener Daten wird im öffentlichen Bereich in der Regel in Bezug auf deren Verwendung in der laufenden Verwaltung diskutiert. Wenn die Daten dort nicht mehr zur Aufgabenerfüllung erforderlich und demgemäß zu löschen sind, ist die Thematik aber dennoch nicht erledigt. Vielmehr sind die öffentlichen Stellen im Land auf der Grundlage des Landesarchivgesetzes (ArchG LSA) verpflichtet, ihre Unterlagen dem zuständigen Archiv anzubieten. Soweit die Unterlagen als archivwürdig übernommen werden, stehen sie der Nutzung nach den Maßgaben des § 10 ArchG LSA zur Verfügung. Der Unterschied zwischen Verwaltungs- und Archivtätigkeit wird in der Praxis leider häufig übersehen.

Da auch in diesem Bereich mit personenbezogenen Daten umgegangen wird, hat der Landesbeauftragte das Landesarchiv besucht. Dabei informierte er sich über die Datenhaltung, die Datenbanken, verschiedene Suchfunktionen und die Berücksichtigung der datenschutzrechtlichen Aspekte bei der externen Präsentation. Besonders wurden der Umgang mit geheimhaltungsbedürftigen Unterlagen, die Übernahme und Verwahrung elektronischer Unterlagen und das Verhältnis des ArchG LSA zum IZG LSA erörtert.

Anlass für eine Novellierung des ArchG LSA war eine Debatte im Landtag zur Frage der Anbietung von Unterlagen des Verfassungsschutzes. Zudem bestand der Bedarf, das Archivrecht den Erfordernissen moderner Informations- und Kommunikationstechnologien anzupassen. In einem Artikelgesetz sollten daher u. a. die Anbietung durch die Verfassungsschutzbehörde, die Übergaben von Daten aus laufend aktualisierten Beständen und weitere Vorgaben zum Schutz des Persönlichkeitsrechts geregelt werden. Der Landesbeauftragte wurde im Entwurfsverfahren frühzeitig beteiligt und hatte in Beratungen und durch umfängliche schriftliche Äußerungen Gelegenheit, datenschutzrelevante Aspekte einzubringen. Viele seiner Anregungen fanden Eingang in den Gesetzestext (vgl. LT-Drs. 6/3482, 6/4084; siehe GVBl. LSA 2015 S. 314).

Von besonderer Bedeutung ist zunächst die Klarstellung im Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt, wonach Unterlagen nach Maßgabe des Archivgesetzes dem zuständigen Archiv anzubieten sind. Ebenfalls wichtig war aus Sicht des Landesbeauftragten, der die Aufgaben des Landesbeauftragten für die Informationsfreiheit in Sachsen-Anhalt wahrnimmt, die Regelung des Verhältnisses zum IZG LSA. Nunmehr wird deutlich zum Ausdruck gebracht, dass die Unterlagen, die bereits vor der Archivierung einem Zugang nach einem der Informationsfreiheitsgesetze offen gestanden haben, auch nach dem Archivrecht zur Verfügung zu stellen sind, und zwar ohne Einhaltung sonst eventuell geltender Schutzfristen. Die Entscheidung über den Zugang trifft das zuständige Archiv in eigener Verantwortung. Dies erfordert eine Würdigung der Ausgangssituation nach Maßgabe und Verfahren des jeweiligen Zugangsgesetzes durch das Archiv. Der Hinweis auf ein „Benehmen

mit der abgebenden Stelle“ stellt klar, dass diese zwar nicht inhaltlich verantwortlich ist, aber das Archiv in Bezug auf fachspezifische Hintergründe unterstützen sollte.

Trotz allem musste der Landesbeauftragte gegenüber dem Landtag auf beachtliche Bedenken hinweisen, die dem eingebrachten Gesetzentwurf noch begegneten. Unter anderem sollten Unterlagen aus Bereichen, die in § 101 Abs. 1 StPO aufgezählt sind (spezielle, in besonderem Maße grundrechtsrelevante Maßnahmen der Ermittlungsbehörden), von der Anbietung ausgenommen werden. Zur Begründung wurde auf die bundesrechtliche Löschungsvorgabe in § 101 Abs. 8 StPO verwiesen. Ein Konflikt ist jedoch nicht gegeben, da die Anbietung gerade an die Löschung anknüpft. Durch die archivrechtliche Anbietungsvorgabe tritt ein neuer Zweck der Datenverwendung auf archivgesetzlicher Grundlage ein (vgl. auch die Parallelregelungen in § 16 Abs. 7 DSG LSA; § 20 Abs. 9 BDSG; § 84 Abs. 6 i. V. m. § 71 Abs. 1 Satz 3 SGB X; § 2 Abs. 4 Bundesarchivgesetz).

Besondere Beachtung war auch der Regelung zu schenken, die die Anbietung des gesamten aktuellen Datenbestandes (im Sinne einer jährlichen Spiegelung) bei solchen automatisierten Verfahren vorsieht, die einer laufenden Aktualisierung unterliegen (siehe § 9b ArchG LSA). Durch diese Aktualisierungen würden Daten überschrieben, die dann nicht mehr recherchiert werden könnten. Es soll verhindert werden, dass elektronische Verwaltungsvorgänge infolge der technischen Entwicklung zunehmend der Archivierung entzogen werden. Im Ergebnis kann die getroffene Regelung jedoch dazu führen, dass lebende Personen und ggf. sensible aktuelle Daten betroffen sind. So könnten z. B. Verdachtsinformationen zu schwerwiegenden Straftaten archiviert werden, obwohl die Daten im laufenden System kurz danach als haltlos entfernt wurden. Wenn der Zeitpunkt der Archivierung vor dieser Erkenntnis liegt, bliebe eine unbescholtene Person als Beschuldigter mit eben diesem Tatvorwurf archiviert. Mit der Überlassung der Daten würde der Anspruch der Betroffenen auf Löschung von der datenschutzrechtlich verantwortlichen Stelle zudem auf das Archiv verlagert. Dies setzt aber voraus, dass dieser überhaupt Kenntnis von der Archivierung der Daten hat. Der Anspruch der Betroffenen auf Auskunft gegenüber dem Archiv ist zudem stark eingeschränkt. Verfassungsrechtlich fundierte Auskunfts- und Löschungsansprüche werden so nicht hinreichend gewährleistet. Es hilft den Betroffenen kaum, dass die Regelung in § 9b erst dann in Kraft treten wird, wenn die informationstechnischen und haushalterischen Voraussetzungen für dessen Umsetzung geschaffen sind.

Der Landesbeauftragte hat das neue Archivrecht auf dem Landesarchivtag im April 2015 näher kommentiert und dabei dem Ministerium für Inneres und Sport empfohlen, eine Handreichung für die Anwender des Gesetzes, etwa in Form von Verwaltungsvorschriften, zu erlassen.

11 Gesundheits- und Sozialwesen

11.1 Gesundheitswesen

Die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 „Stärkung des Datenschutzes im Sozial- und Gesundheitswesen“ (**Anlage 4**) weist auf den verschärfenden Wettbewerb der Beteiligten im Sozial- und Gesundheitswesen hin. Dadurch geraten die Rechte der Patien-

tinnen und Patienten und Versicherten immer stärker unter Druck. Durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von „gläsernen Patientinnen und Patienten oder Versicherten“ weiter verstärkt. Demgemäß appelliert die Konferenz der Datenschutzbeauftragten an die Regierungen und Parlamente des Bundes und der Länder, sich für die Entwicklung datenschutzfreundlicher Technologien, eine vertrauliche und zuverlässige Telematikinfrastruktur sowie hinreichende gesetzliche Regelungen zum Einsatz externer Dienstleister einzusetzen (vgl. dazu auch Nr. 11.1.3).

11.1.1 Krankengeldfallmanagement

Erkrankt ein Arbeitnehmer und führt die Krankheit zur Arbeitsunfähigkeit oder wird ein Versicherter auf Kosten der Krankenkasse stationär in einem Krankenhaus, einer Vorsorge- oder Rehabilitationseinrichtung behandelt, so erhält er gemäß § 44 SGB V i. V. m. § 3 Abs. 1 Satz 1 Entgeltfortzahlungsgesetz von seiner gesetzlichen Krankenkasse nach sechs Wochen Krankengeld. Die Krankenkassen möchten die Versicherten bei der Reintegration in das Arbeitsleben unterstützen und setzen auf umfassende Beratung und Unterstützung des Versicherten – im Rahmen eines Krankengeldfallmanagements. Ob sich die Krankenkassen dabei immer auf dem datenschutzrechtlich vorgesehenen Weg befinden, ist gelegentlich fraglich. Bereits in seinem XI. Tätigkeitsbericht (Nr. 10.1.6) hat der Landesbeauftragte in Bezug auf Krankenhausentlassungsberichte das Thema Krankengeldfallmanagement aufgegriffen. Zahlreiche Hinweise auf datenschutzrechtlich bedenkliches Verhalten von Krankenkassen in Bezug auf Krankengeld ergaben sich aus den Tätigkeitsberichten anderer Datenschutzbeauftragter des Bundes und der Länder.

Eine erste Kontrolle zum Krankengeld bei einer Krankenkasse mit Einsichtnahme in Fallakten führte zu folgenden Feststellungen: Die geprüfte Krankenkasse lässt sich standardmäßig von Versicherten eine Einwilligungserklärung unterzeichnen, dass von der Krankenkasse medizinische Daten über sie von den Ärzten und Einrichtungen eingeholt werden können, die bei der Behandlung der Arbeitsunfähigkeit mitgewirkt haben. Gleichzeitig entbanden die Versicherten die behandelnden Ärzte und schweigepflichtigen Mitarbeiter von Einrichtungen insoweit von der Schweigepflicht. Die Krankenkasse nutzt die Erklärungen, um anschließend (häufig von allen angegebenen Ärzten und Einrichtungen wie Krankenhäusern und Rehabilitationseinrichtungen) Arztberichte und Krankenhaus- oder Rehabilitationsentlassungsberichte anzufordern. In einigen Fällen wurden Vordrucke handschriftlich ergänzt und Ärzte z. B. um ausführliche Hausarztbefunde mit Kopien der Epikrise von stationären Aufenthalten und Entlassungsberichte von Rehabilitationseinrichtungen gebeten. Teilweise lagen den geprüften Fallakten ärztliche Entlassungsberichte mit ausführlichen Krankheitsbeschreibungen, Kopien von Befunden, z. B. von Endoskopien bei. Die Unterlagen befanden sich offen in den Fallakten.

Es kann bezweifelt werden, dass dem Versicherten bewusst ist, in welchem Umfang die Krankenkasse medizinische Daten über ihn auf der Grundlage seiner Erklärungen sammelt. Überdies stellt sich die Frage, ob und wozu die Erhebung medizinischer Daten auf der Grundlage einer Einwilligungserklärung für die Krankenkasse erforderlich ist. Erforderlich für die Krankenkasse wären die Daten dann, wenn sie für

die Prüfung der Leistungsvoraussetzungen notwendig sind. Dies kann bei medizinischen Daten jedoch bezweifelt werden. Krankenkassen sind verpflichtet, bei Arbeitsunfähigkeit eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung (MDK) einzuholen, um den Behandlungserfolg zu sichern oder Zweifel an der Arbeitsunfähigkeit zu beseitigen (§ 275 Abs. 1 Satz 1 Nr. 3 SGB V). Dabei kann die Krankenkasse (nur dann) von einer Beauftragung des MDK absehen, wenn sich die medizinischen Voraussetzungen der Arbeitsunfähigkeit eindeutig aus den der Krankenkasse vorliegenden ärztlichen Unterlagen ergeben (§ 275 Abs. 1 Satz 4 SGB V).

Auf welche ärztlichen Unterlagen kann aber die Krankenkasse zur Prüfung der Arbeitsunfähigkeit zurückgreifen? Hier steht ihr die Arbeitsunfähigkeitsbescheinigung zur Verfügung, mit der der behandelnde Arzt über Beginn und voraussichtliche Dauer sowie die die Arbeitsunfähigkeit verursachenden Diagnosen informiert. Hat sie danach Zweifel an der Arbeitsunfähigkeit, ist sie verpflichtet, den MDK einzubeziehen. Dies liegt darin begründet, dass es sich bei den Mitarbeitern anders als bei Gutachtern des MDK um „medizinisch nicht besonders ausgebildete Mitarbeiter der Krankenkasse“ handelt (so ausdrücklich Bundessozialgericht, Urteil vom 16. Mai 2012, Az. B 3 KR 12/11 R, juris). Die Krankenkassen dürfen keine Einsicht in die Behandlungsunterlagen der Versicherten nehmen, sondern sind aus Gründen des Sozialdatenschutzes auf das Tätigwerden des MDK angewiesen. Sofern Krankenkassen darauf hinweisen, nach § 284 Abs. 1 Nr. 7 SGB V für eine Beteiligung des MDK Sozialdaten erheben zu dürfen, ist klarzustellen, dass dies nur die Datenerhebung zur Entscheidung betrifft, ob der MDK einzubeziehen ist, also Zweifel an der Arbeitsunfähigkeit bestehen. Dies können z. B. auffällige Häufungen von Arbeitsunfähigkeiten, auffällig häufige, aber nur kurzzeitige Arbeitsunfähigkeiten, ein häufiger Beginn der Arbeitsunfähigkeit am Beginn oder Ende der Woche sein. Die Erhebung medizinischer Daten ist hier nicht gemeint. Nach der inzwischen gefestigten Rechtsprechung dürfen die Krankenkassen keine medizinischen Unterlagen zur Vorprüfung anfordern (Bundessozialgericht, Urteil vom 23. Juli 2002, Az. B 3 KR 64/01 R, juris; Urteil vom 16. Mai 2012, Az. B 3 KR 14/11 R, juris).

Darüber hinaus hat das Bundessozialgericht Zweifel geäußert, ob Einwilligungen im Bereich der gesetzlichen Krankenversicherung überhaupt freiwillig sein können. Eine Datennutzung kraft Einwilligung jedenfalls im Bereich der gesetzlichen Krankenversicherung sei nicht pauschal, sondern nur in ausdrücklich normierten Fällen zuzulassen (Urteil vom 10. Dezember 2008, Az. B 6 KA 37/07 R, juris). Für die Übermittlung medizinischer Daten im Rahmen des Fallmanagements an Krankenkassen bleibt somit kein Raum, auch nicht bei Vorliegen einer Einwilligungserklärung.

Dass sich medizinische Unterlagen der Versicherten in den Fallakten der Krankengeldfallmanager der Krankenkasse befinden, ist daher äußert kritisch zu sehen. Das Prüfverfahren bei der geprüften Krankenkasse ist noch nicht abgeschlossen und wird den Landesbeauftragten noch einige Zeit beanspruchen (siehe auch Nr. 11.1.2).

11.1.2 GKV-Versorgungsstärkungsgesetz

Mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung sollen u. a. eine flächendeckende und gut erreichbare Versorgung sichergestellt, der Zugang der Versicherten zur Versorgung beschleunigt und

Leistungsansprüche verbessert werden. Eine Änderung des § 44 SGB V sieht vor, dass Versicherte Beratung und Hilfe der Krankenkassen in Bezug auf Wiederherstellung der Arbeitskraft beanspruchen können. Die dazu erforderlichen Daten sollten sie nach Aufklärung und Einwilligung erheben und verarbeiten dürfen. Hiergegen bestehen Bedenken, dass diese Regelung der ausdifferenzierten Verteilung der Verarbeitungskompetenzen zwischen den Krankenkassen und dem MDK gemäß §§ 275, 276 SGB V widerspricht. Danach sollen die Krankenkassen gerade keine detaillierten Daten über den Gesundheitszustand der Versicherten sammeln dürfen. Auch gegen die Nutzung der Einwilligung bestehen systematische und im Hinblick auf das Prinzip der Freiwilligkeit materielle Bedenken (siehe auch Nr. 11.1.1).

Hierzu fasste die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. Dezember 2014 die Entschließung „Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!“ (**Anlage 20**). Bei dem derzeit praktizierten Krankengeldfallmanagement lade eine Vielzahl von Krankenkassen ihre Versicherten bei einer Arbeitsunfähigkeit frühzeitig zu einem persönlichen Gespräch ein und stelle Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Bisheriges datenschutzrechtlich problematisches Vorgehen dürfe nicht gestützt werden. In der Fassung des Gesetzentwurfs (BT-Drs. 18/4095) wurde die Problematik lediglich in der Begründung verbal korrigiert, indem auf das Ende der Hilfe und Beratung hingewiesen wurde, wenn die Krankenkassen den MDK einschalten müssen. Die insofern unverändert gebliebene Regelung ist Teil des Gesetzes vom 16. Juli 2015 (BGBl. I S. 1211).

11.1.3 Elektronische Gesundheitskarte

Bereits im IX. (Nr. 12.1) und X. Tätigkeitsbericht (Nr. 12.2) berichtete der Landesbeauftragte über die Einführung der elektronischen Gesundheitskarte (eGK). Seit dem 1. Januar 2014 ist die eGK in Deutschland flächendeckend durch die Krankenkassen ausgegeben worden. Seit dem 1. Januar 2015 gilt ausschließlich die eGK als Berechtigungsnachweis, um Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen zu können.

Nach Diskussionen auf politischer Ebene regelte der Gesetzgeber in § 291a SGB V, dass die eGK geeignet sein muss, Hinweise von Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebsspende aufzunehmen. In die derzeit ausgegebene Karte ist die Aufnahme der vollen Erklärung allerdings technisch nicht möglich; die Umsetzung dürfte damit frühestens in ein paar Jahren möglich sein. Datenschutzrechtlich relevant ist die Umsetzung der Authentifizierung eines Patienten bei der Abgabe oder Änderung der Organspendeerklärung. Die Authentifizierung sollte über die Eingabe einer Multireferenz-PIN gewährleistet werden. Dies war aus Sicht des Datenschutzes jedoch nicht ausreichend, da der Gesetzeswortlaut des § 291a Abs. 3 Satz 2 SGB V offensichtlich eine Authentifizierung verlangt, die über den normalen Schutz, den die eGK liefert, hinausgeht.

Die gegen die Vorlage eines Lichtbildes für die eGK vorgetragenen datenschutzrechtlichen Bedenken wurden in mehreren Gerichtsverfahren überprüft. Inzwischen hat das Bundessozialgericht (Urteil vom 18. November 2014, Az. B 1 KR 35/13 R, juris) bestätigt, dass Versicherte keinen Anspruch auf Zurverfügungstellung einer Nachweisberechtigung entsprechend der zuvor gültigen Krankenversicherungskarte

ohne Lichtbild und eGK-Chip anstelle der eGK haben. Das Grundrecht auf informationelle Selbstbestimmung sei nicht verletzt. Die eGK sei in ihrer gegenwärtigen Gestalt und ihren gegenwärtigen und zukünftigen Pflichtangaben und Pflichtanwendungen durch überwiegende Allgemeininteressen gerechtfertigt. Die eGK verbessere den Schutz vor missbräuchlicher Inanspruchnahme von Leistungen der gesetzlichen Krankenversicherung und fördere auch im Übrigen die Wirtschaftlichkeit der Leistungserbringung. Die freiwilligen, vom Einverständnis der Betroffenen abhängigen Anwendungen der eGK begegnen keinen verfassungsrechtlichen Bedenken. Das Recht schütze bereits die betroffenen Daten vor unbefugtem Zugriff Dritter und vor missbräuchlicher Nutzung. Dass die Datensicherheit faktisch unzulänglich sei, ließe sich zudem zurzeit nicht feststellen, da sich die Telematikinfrastruktur noch im Teststadium befinde.

Zuständig für Umsetzungen ist die Gematik als Beteiligungsunternehmen der Spitzenorganisationen des deutschen Gesundheitswesens, 2005 mit dem Ziel errichtet, die Telematikinfrastruktur im Gesundheitswesen, die eGK und die zugehörigen Telematikanwendungen einzuführen, zu pflegen und weiterzuentwickeln. Gegenstand einer Erprobung sollte vor allem das Versicherten-Stammdatenmanagement sein; darüber hinaus sollten die Anbindung an und die Nutzung von sicheren Bestandsnetzen und der freie Internetzugang erprobt werden. Zwischenzeitlich wurde der Start der Erprobung auf Ende 2014 und dann auf Herbst 2015 verschoben. An der Erprobung sollen nun in zwei Testregionen je 500 Ärzte, Zahnärzte, Psychotherapeuten und fünf Krankenhäuser teilnehmen. Dabei sollen alle real vorkommenden Geschäftsfälle des Versichertenstammdaten-Managements sowie die Anwendung der qualifizierten elektronischen Signatur für die sichere Kommunikation zwischen Ärzten erprobt werden. Die Erprobung werde durch eine wissenschaftliche Evaluation begleitet, die Fragen der Akzeptanz und Praxistauglichkeit bewerten solle. Hier ist Sachsen-Anhalt nicht als Testregion einbezogen. Die sichere Einbindung künftiger Anwendungen in die Telematikinfrastruktur wird in den zuständigen Gremien beraten, in denen die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und auch einige Landesbeauftragte für den Datenschutz sowie das Bundesamt für Sicherheit in der Informationstechnik eingebunden sind.

Mit dem Referentenentwurf für ein Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (**„eHealth-Gesetz“**) vom Januar 2015 sind verbindliche Termine festgelegt, zu dem Ärzte und Krankenkassen in der Lage sein müssen, elektronisch die Versicherten-Stammdaten auszutauschen (30. Juni 2016) oder zu dem Ärzte den Notfalldatensatz auf der eGK eintragen können müssen (1. Januar 2018). Die Telematikinfrastruktur als zentrale elektronische Infrastruktur im Gesundheitswesen soll aufgebaut und zügig die Einführung und Nutzung medizinischer und administrativer Anwendungen erfolgen. Mit der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 „Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich“ (**Anlage 24**) wird zu weiteren Verbesserungen aufgefordert. Hinsichtlich der Telematikinfrastruktur seien die Wahrung der Transparenz und die Wahrnehmung der Rechte der Betroffenen zu stärken. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sollten im Verfahren neben Technikexperten auch Datenschutzexperten hingezogen werden. Weiter müsse der Bundesgesetzgeber klare Rahmenbedingungen für die Einschal-

tung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen.

Der durch das Gesetz vom 21. Dezember 2015 (BGBl. I S. 2408) entstehende Zeitdruck darf nicht zur Vernachlässigung der Anforderungen technischer und organisatorischer Datensicherheit führen. Patientengeheimnis und medizinische Funktionalität müssen in Einklang gebracht werden. Datenschutzrechtliche Forderungen dürfen bei der Verbesserung der Qualität und Wirtschaftlichkeit der medizinischen Versorgung nicht außer Acht gelassen werden.

11.1.4 Medizinischer Dienst der Krankenversicherung

Der Landesbeauftragte hat im Berichtszeitraum den Medizinischen Dienst der Krankenversicherung Sachsen-Anhalt (MDK) einer Kontrolle unterzogen. Bereits im VII. Tätigkeitsbericht (Nr. 20.15) hat sich der Landesbeauftragte mit der Frage der Zulässigkeit des Outsourcings des Schreibdienstes beschäftigt. Dabei hat er festgestellt, dass es sich bei dem Verfahren um grundsätzlich zulässige Datenverarbeitung im Auftrag nach § 80 SGB X handelt. Wesentlich ist jedoch, dass die in den sozialmedizinischen Gutachten enthaltenen sensiblen personenbezogenen Daten nicht nur dem Sozialdatenschutz, sondern auch dem besonderen strafrechtlichen Schutz des Patientengeheimnisses nach § 203 StGB unterliegen. Die Angestellten des externen Schreibdienstes können nicht wie z. B. die angestellten Arzthelferinnen als berufsmäßig tätige Gehilfen im Sinne des § 203 Abs. 3 StGB angesehen werden. Die Offenbarung von Patientengeheimnissen bedarf deshalb einer Befugnis in Form einer Einwilligungs- bzw. Schweigepflichtentbindungserklärung der betroffenen Patienten. Der MDK erarbeitete in Abstimmung mit dem Landesbeauftragten seinerzeit eine Einwilligungserklärung zur Einschaltung eines externen Schreibdienstes.

Im Rahmen der nunmehr durchgeführten Prüfung stellte der Landesbeauftragte fest, dass bei fehlendem Patientenkontakt, z. B. bei Gutachten nach Aktenlage, eine Einverständniserklärung und Schweigepflichtentbindung des Patienten nicht eingeholt wurde, die Gutachten jedoch trotzdem durch den externen Schreibdienst gefertigt wurden. Der Landesbeauftragte wies den MDK auf die datenschutzrechtliche Unzulässigkeit und den Verstoß gegen die Verschwiegenheitspflichten des § 203 Abs. 1 StGB durch die begutachtenden Ärzte hin. Der MDK teilte in einer Stellungnahme mit, Begutachtungen nach Aktenlage seien ein wichtiger Baustein der Arbeit des MDK. Über 23.000 Kassenaufträge begutachte der MDK ohne Versichertenkontakt; ein Großteil der Gutachten werde durch den externen Dienstleister geschrieben. Die Information des Versicherten stelle einen unverhältnismäßigen Aufwand dar. Demgegenüber erläuterte der Landesbeauftragte, dass auch der Aspekt der Begutachtung nach Aktenlage ohne Versichertenkontakt die Beurteilung nicht zu ändern vermag. Zwar sind die medizinischen Daten des Versicherten dem Gutachter dann nicht persönlich anvertraut worden. § 203 StGB spricht jedoch davon, dass die Daten dem Arzt in seiner Eigenschaft anvertraut oder sonst bekannt geworden sind. Demgemäß reicht eine Kenntniserlangung in Ausübung der beruflichen Eigenschaft und Funktion aus. Eine Kenntniserlangung des Offenbarenden auch ohne persönlichen Vertrauensakt wird ebenfalls von § 203 StGB erfasst, etwa durch Mitteilung eines Dritten. Diese Beziehung kann daher auch dann bestehen, wenn sie unfreiwillig entstanden ist, wie u. U. beim Amtsarzt oder gerichtlich bestellten Gutachter. Der ärztliche Gutachter des MDK, der medizinische Versichertendaten lediglich aus Akten eines

Krankenhauses oder anderen Arztes erhält und keinen Versichertenkontakt hat, ist daher auch in die strafrechtliche Sanktion des § 203 StGB eingebunden.

Der MDK blieb bei seiner Auffassung, da der Schreibdienst als Auftragnehmer nach § 80 SGB X ja nicht „Dritter“ sei, dem Daten offenbart würden. Da der Schreibdienst lediglich infolge der Fiktion des § 80 SBB X kein „Dritter“ im datenschutzrechtlichen Sinn ist (Auftragnehmer), führt dies allerdings nur zur datenschutzrechtlichen Zulässigkeit. Eine Offenbarungsbefugnis nach § 203 StGB wird jedoch nicht begründet. Der Landesbeauftragte hat deshalb das Ministerium für Arbeit und Soziales als Aufsichtsbehörde (§ 90 Abs. 2 SGB IV) über die Rechtsauffassung des MDK informiert.

Eine weitere Auffälligkeit im Rahmen der Prüfung ergab sich zu dem Verfahren, über das der MDK die für die Begutachtung erforderlichen Unterlagen erhält. Der MDK ging davon aus, dass die Krankenkassen die für die Begutachtung erforderlichen Unterlagen bei den Leistungserbringern, z. B. Ärzten, mit dem Hinweis anfordern, dass diese direkt an den MDK zu senden sind. Sofern Unterlagen der Leistungserbringer durch die Kassen eingereicht werden, seien diese allerdings nur größtenteils, aber nicht in allen Fällen in Umschlägen mit dem Vermerk „nur vom MDK zu öffnen“ enthalten. Eigene Prüfungen des Landesbeauftragten bei einer Krankenkasse ergaben zudem, dass medizinische Befundunterlagen, die für den MDK angefordert wurden, dort offen, d. h. ohne Umschlag, in den Krankengeldakten vorlagen (siehe Nr. 11.1.1).

Grundsätzlich sind Sozialdaten nach § 276 Abs. 2 Satz 1 2. Halbsatz SGB V unmittelbar an den MDK zu übermitteln, soweit dies für die gutachterliche Stellungnahme und Prüfung erforderlich ist. Der MDK als datenerhebende verantwortliche Stelle (§ 67 Abs. 9 Satz 1 SGB X) muss sicherstellen, dass die Sozialdaten nur Personen zugänglich sind, die sie zur Erfüllung ihrer Aufgaben benötigen. Bei einer Einbeziehung von Krankenkassen in die Datenerhebung wäre durch den MDK sicherzustellen, dass die Anforderungen der Krankenkassen den rechtlichen Vorgaben entsprechen. Da sich der den Krankenkassen zukommende medizinische Datenbestand nach den Vorgaben des SGB V beschränkt (vgl. § 301 Abs. 1 SGB V) und nur diese Unterlagen unter die Vorlagepflicht der Krankenkassen nach § 276 Abs. 1 Satz 1 SGB V fallen, wäre nur ein Verfahren datenschutzrechtlich akzeptabel, das sicherstellt, dass die Krankenkassen die weitergehenden medizinischen Daten nicht offen zur Kenntnis erhalten. Das bisherige Verfahren, dass Krankenkassen den MDK unterstützen, indem sie Unterlagen bei den Leistungserbringern für den MDK anfordern, ist nur unter der Voraussetzung akzeptiert worden, dass die medizinischen Unterlagen in einem verschlossenen und verschlossen bleibenden Umschlag an den MDK durchgereicht werden. Der MDK wurde aufgefordert, mit für ein datenschutzkonformes Erhebungsverfahren Sorge zu tragen.

11.1.5 Versand von Gutachten durch den Medizinischen Dienst der Krankenversicherung

Mehrere Petenten beschwerten sich im Zusammenhang mit der Gutachtenerstellung des Medizinischen Dienstes der Krankenversicherung (MDK) über dessen Verhalten. Sie gaben an, ein Einverständnis zur Übermittlung des vollständigen ärztlichen Gutachtens an die Krankenkasse ausdrücklich nicht gegeben zu haben. Trotzdem sei der Krankenkasse das vollständige Gutachten zugeleitet worden.

Der MDK erklärte in seinen Stellungnahmen, dass jeder Versicherte vor Beginn der Begutachtung sein Einverständnis zur Datenübermittlung an die Krankenkasse und den behandelnden Arzt erteilen müsse. Bei den vorliegenden Gutachten sei aus Versehen in der genutzten Software der Medizinischen Dienste „Ismed“ bei den Versandeinstellungen „alles“ ausgewählt worden. Der MDK entschuldigte sich für das Versehen und gab an, die Vorfälle zum Anlass zu nehmen, um die Gutachter für den Umgang mit der Datenübermittlung zu sensibilisieren. Zusätzlich seien für alle Gutachtenprodukte die Versandeinstellung „ohne Befund“ und „ohne Anamnese“ EDV-technisch als Grundeinstellungen eingerichtet worden.

Die Sensibilisierung der Gutachter wurde ausdrücklich begrüßt. Zu seinen Mitteilungspflichten wurde der MDK jedoch auf § 277 SGB V hingewiesen. § 277 Abs. 1 SGB V stellt bereits eine gesetzliche Befugnis für die Übermittlung des Ergebnisses der Begutachtung dar. Der MDK hat der Krankenkasse und dem Arzt oder sonstigen Leistungserbringer, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, das Ergebnis der Begutachtung zu übermitteln. Der Krankenkasse hat er darüber hinaus die erforderlichen Angaben über den Befund mitzuteilen (§ 277 Abs. 1 Satz 1 SGB V). Da eine gesetzliche Übermittlungsbefugnis besteht, bedarf es keiner Einverständniserklärung des Versicherten. Weitere Übermittlungsbefugnisse sind dem MDK gesetzlich nicht eingeräumt. Diese klar abgrenzende Ausgestaltung bedeutet, dass der MDK weitere Angaben, z. B. ein vollständiges Gutachten, auf der Grundlage einer Einwilligungserklärung nicht übermitteln darf. Die Vorgabe des Gesetzgebers darf der MDK nicht mit Hilfe einer Einverständniserklärung unterlaufen.

Der MDK hat daraufhin erklärt, diese Einverständniserklärungen nicht mehr einzuholen. Die Gutachter seien darauf hingewiesen worden, dass die Gutachten nur die notwendigen Angaben zur Beantwortung der Fragen der Kassen beinhalten.

Die Eingaben nahm der Landesbeauftragte zum Anlass, die Umsetzung der Maßnahmen zu überprüfen. Er hat festgestellt, dass der MDK die Standard-Versandeinstellungen geändert hat. Voreingestellt sind nunmehr „ohne Vorgeschichte und Anamnese“ sowie „ohne Befund“. Erforderliche Angaben über den Befund, die die Krankenkasse für die Entscheidung über die Leistungsgewährung benötigt, sind durch die Gutachter unter „sozialmedizinische Begründung“ einzutragen. Der Landesbeauftragte beriet den MDK dahingehend, dass es im Hinblick auf die Erfahrungen in anderen Bundesländern geboten erscheint, die konsequente Einhaltung der neuen Verfahren regelmäßig strukturiert zu kontrollieren. Insbesondere ist die Gefahr zu berücksichtigen, dass Gutachter zur Vereinfachung schlicht das gesamte Gutachten in das neue Feld „sozialmedizinische Begründung“ kopieren. Der MDK teilte mit, dies durch verschiedene Maßnahmen sicherzustellen (Dienstanweisung, Qualitätssicherung, internes Audit).

Bei der Ergebnisübermittlung an Leistungserbringer können nach § 277 Abs. 1 SGB V erforderliche Angaben über den Befund ebenfalls mitgeteilt werden. Der Versicherte kann dem widersprechen, worauf er rechtzeitig hinzuweisen ist. Im Rahmen der Prüfung ergab sich, dass bei Fällen, in denen eine Begutachtung ohne Versichertenkontakt stattfindet, eine Information der Betroffenen über ihr Widerspruchsrecht nicht erfolgte. Dies sei nach Ansicht des MDK nicht handhabbar. Der MDK wies weiter auf technische Probleme hin. Die Wahrnehmung seines Rechts auf Widerspruch nach § 277 Abs. 1 Satz 3 SGB V durch den Versicherten setzt jedoch voraus, dass er Kenntnis von der Begutachtung und vom beabsichtigten Datenfluss haben und

sein Recht auf Widerspruch kennen muss. Daher wurde dem MDK erläutert, dass es notwendig ist, entweder von einer Übersendung der Daten an den Leistungserbringer abzusehen oder die Information des Versicherten sicherzustellen, um sein Recht auf Widerspruch zu wahren. Alternativ käme eine postalische Versendung eines Ergebnisausdrucks in Betracht.

11.1.6 Prüfung der Krankenhausabrechnung

Ein Krankenhaus wandte sich an den Landesbeauftragten, da Krankenkassen immer häufiger medizinische Begründungen dafür verlangen würden, warum die Versorgung eines Versicherten stationär erfolgen musste. Gegen die Übermittlung von patientenbezogenen medizinischen Sachverhalten außer denen, die in § 301 SGB V genannt sind, hege das Krankenhaus aus datenschutzrechtlichen Gründen Bedenken. Im Zuge von Abrechnungsprüfungen nach §§ 275, 276 SGB V fordere der Medizinische Dienst der Krankenversicherung (MDK) umfangreiche patientenbezogene Unterlagen an, die nach Auffassung des Krankenhauses für die Beantwortung der von den Krankenkassen angegebenen konkreten Fragestellung nicht notwendig seien.
Grundsätzlich sind die Krankenkassen z. B. bei der Erbringung von Leistungen verpflichtet, insbesondere zur Prüfung von Voraussetzungen, Art und Umfang der Leistung sowie bei Auffälligkeiten zur Prüfung der ordnungsgemäßen Abrechnung eine gutachterliche Stellungnahme des MDK einzuholen (§ 275 Abs. 1 Nr. 1 SGB V). Da Krankenkassen als Sozialversicherungsbehörden in aller Regel nicht über ausreichenden medizinischen Sachverstand verfügen, obliegt die Leistungsüberprüfung und damit auch die Prüfung von Krankenhausabrechnungen in medizinischer Hinsicht dem MDK. Daraus folgt, dass die Krankenkassen selbst keine medizinischen Erhebungen durchführen und von den Leistungserbringern auch keine entsprechenden Auskünfte einholen dürfen. Ausnahmen bestehen nur bezüglich medizinischer Begründungen bei Überschreitung der voraussichtlichen Dauer der Krankenhausbehandlung (§ 301 Abs. 1 Nr. 3 letzte Alt. SGB V) oder entsprechenden Regelungen in den Landesverträgen nach § 112 SGB V, die in Sachsen-Anhalt jedoch nicht bestehen.

Im Verhältnis zwischen Krankenhäusern, Krankenkassen und den Medizinischen Diensten bestehen nach ständiger Rechtsprechung des Bundessozialgerichts Auskunfts- und Prüfpflichten auf drei Ebenen (Bundessozialgericht, Urteil vom 16. Mai 2013, Az. B 3 KR 32/12 R, juris).

Auf der *ersten Stufe* sind zunächst zwingend die Angaben nach § 301 Abs. 1 SGB V zu machen. Danach besteht die Pflicht des Krankenhauses, der Krankenkasse die wesentlichen Aufnahme- und Behandlungsdaten zu übermitteln. Aus datenschutzrechtlichen Gründen ist abschließend und enumerativ aufgelistet, welche Angaben der Krankenkasse auf jeden Fall zu übermitteln sind (vgl. BT-Drs. 12/3608, S. 124). Nach der zugrunde liegenden Vorstellung des Gesetzgebers sind damit die Mindestangaben bezeichnet, die die Krankenkasse insbesondere zur ordnungsgemäßen Abrechnung und zur Überprüfung der Notwendigkeit der Krankenhausbehandlung benötigt.

Genügt die Anzeige des Krankenhauses diesen (Mindest-)Anforderungen nicht, dürfen die Krankenkassen bei Zweifeln oder Unklarheiten in Bezug auf die gemäß § 301 SGB V übermittelten Daten durch (nicht-medizinische) Nachfragen beim Kranken-

haus selbst klären, ob die jeweiligen Voraussetzungen der Zahlungspflicht im Einzelfall gegeben sind. So hat das Bundessozialgericht bereits entschieden, dass zum nach § 301 SGB V anzugebenden Grund der Aufnahme auch Angaben dazu zu machen sind, warum eine im Regelfall ambulant durchzuführende bzw. ambulant mögliche Versorgung im konkreten Einzelfall stationär vorgenommen worden ist. Die gegenseitigen Verpflichtungen in der Dauerbeziehung zwischen Krankenkasse und Krankenhaus bedingen, dass das Krankenhaus bei ihm verfügbare und für die Prüfung der Krankenhausabrechnung erforderliche Informationen weitergibt. Eine Krankenhausrechnung ist grundsätzlich nur dann schlüssig, wenn ihr im Sinne von § 301 Abs. 1 Nr. 3 SGB V ausreichende Angaben zum Grund der stationären Leistungserbringung beigegeben wurden (Bundessozialgericht, Urteil vom 21. März 2013, Az. B 3 KR 28/12 R, juris). Die anschließende Prüfung indes, ob die vom Krankenhaus genannten Gründe vorliegen und medizinisch stichhaltig sind, bleibt allein dem MDK vorbehalten.

Erschließt sich die Notwendigkeit der Krankenhausbehandlung oder weiterer Abrechnungsvoraussetzungen den medizinisch nicht besonders ausgebildeten Mitarbeitern der Krankenkasse aufgrund der Angaben nach § 301 SGB V nicht selbst, sind weitere medizinische Ermittlungen ausschließlich auf der *zweiten Stufe* der Sachverhaltserhebung zulässig. Das bedeutet, dass ein Prüfverfahren nach § 275 Abs. 1 Nr. 1 SGB V einzuleiten ist. Dazu hat die Krankenkasse dem MDK nach § 276 Abs. 1 Satz 1 SGB V diejenigen zur Begutachtung erforderlichen Unterlagen vorzulegen, die ihr vom Krankenhaus zur Verfügung gestellt worden sind, also insbesondere die Angaben nach § 301 SGB V. Hinzu kommen ggf. vom Versicherten überlassene Unterlagen bei dessen Zustimmung (§ 276 Abs. 1 Satz 2 SGB V). Den Krankenkassen steht auch in diesem Stadium kein Recht zu, selbst in die ärztlichen Behandlungsunterlagen Einsicht zu nehmen.

Im Rahmen einer ordnungsgemäß eingeleiteten Prüfung hat das Krankenhaus schließlich auf der *dritten Stufe* der Sachverhaltsaufklärung dem MDK auch über die Anzeige nach § 301 SGB V hinaus alle weiteren Angaben zu erteilen und Unterlagen vorzulegen, die im Einzelfall zur Beantwortung der Prüfanfrage der Krankenkasse bzw. des MDK benötigt werden. Die Leistungserbringer sind verpflichtet, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. Rechtsgrundlage hierfür ist § 276 Abs. 2 Satz 1, 2. Halbsatz SGB V. In Betracht kommen die Übersendung der gesamten Krankenakte, von Teilen hiervon, das Einholen von Auskünften bei behandelnden Ärzten oder die Einsichtnahme in Krankenunterlagen vor Ort nach § 276 Abs. 4 Satz 1 SGB V. Begrenzt wird diese Auskunfts- bzw. Herausgabepflicht durch den dem Krankenhaus mitzuteilenden Prüfgrund, aus dem sich auch die konkrete Aufgabe des MDK ergibt.

Die Anforderung von Behandlungsunterlagen durch den MDK ist ordnungsgemäß zu begründen. Das ist aus dem Rechtsgedanken des § 35 SGB X abzuleiten, der im Hinblick auf die Pflichtenstellung des Inhabers von Krankenbehandlungsunterlagen auch in diesem Zusammenhang Geltung beansprucht. Der Inhaber der Krankenunterlagen ist im Verhältnis zu seinen Patienten aus dem zugrunde liegenden Behandlungsvertrag und zur Meidung strafrechtlicher Sanktionen nach § 203 Abs. 1 Nr. 1 StGB gehalten, die Berechtigung der Anforderung selbst zu prüfen. Dazu sind diejenigen Gründe anzugeben, aus denen der Adressat die für die Anforderungen leitenden Gründe entnehmen kann; das hat auch der MDK zu beachten (Bundessozialge-

richt, Urteil vom 22. April 2009, B 3 KR 24/07 R, juris). Trotz seiner Prüfpflicht, ob die Weitergabe erforderlich und damit zulässig ist, darf das Krankenhaus die Anforderung von Unterlagen ohne substantiierten Hinweis auf bereits vorliegende, eine zuverlässige Beurteilung ermöglichende Unterlagen nicht formelhaft ablehnen oder grundlos schlechthin verweigern (Bundessozialgericht vom 22. April 2009, a. a. O.).

Vor diesem rechtlichen Hintergrund hat der Landesbeauftragte die Problematik mit dem Krankenhaus erörtert. Die Fragestellungen wurden in eine Prüfung und Beratung des MDK (siehe Nr. 11.1.4) mit dem Ziel der Konkretisierung der Anfragen unter Erforderlichkeitsaspekten einbezogen.

11.1.7 Krankenhausinformationssysteme

Der Landesbeauftragte hatte bereits in den vorigen Tätigkeitsberichten (X. Tätigkeitsbericht, Nr, 12.1, und XI. Tätigkeitsbericht, Nr. 10.1.1) auf die Orientierungshilfe Krankenhausinformationssysteme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen. Er weist auch weiterhin in Beratungen gegenüber Krankenhäusern auf die Maßstäbe der Orientierungshilfe für den Umgang mit Patientendaten hin.

Inzwischen haben die Datenschutzbeauftragten die Orientierungshilfe mit dem Ziel besserer Handhabbarkeit überarbeitet. Dabei flossen vielfältige Anregungen aus dem Bereich der überprüften und beratenen Krankenhäuser ebenso ein wie Rückmeldungen aus einem Austausch mit Krankenhausgesellschaften sowie anderen Beteiligten. Die Orientierungshilfe verdeutlicht rechtliche Anforderungen, berücksichtigt stärker landesrechtliche Besonderheiten und betont die Freiräume der Krankenhäuser bei der Ausgestaltung ihrer Informationssysteme. Die Zusammenhänge zwischen rechtlichen und technischen Anforderungen werden erklärt.

Ergänzend wurde für einrichtungs- und mandantenübergreifende Zugriffe (z. B. Zusammenarbeit mit Medizinischen Versorgungszentren) ein Szenarienkatalog entwickelt. Die Konferenz hat die Orientierungshilfe in der aktuellen Fassung im März 2014 zustimmend zur Kenntnis genommen. Sie steht auf der Homepage des Landesbeauftragten zur Verfügung.

11.1.8 Patientenidentifikation mittels Patientenarmbändern

Aufgrund eines Presseartikels zum Thema Patientenarmbänder wurde der Landesbeauftragte auf diese Angelegenheit aufmerksam. Patientenarmbänder dienen während eines klinischen Aufenthaltes der sicheren Identifikation von Patienten. Dafür erhält der Patient bei der Aufnahme ein Armband, auf dem ein bestimmter Datensatz gespeichert ist. Um zu erfahren, ob und wie Patientenarmbänder in Sachsen-Anhalt Anwendung finden, hat der Landesbeauftragte sieben Krankenhäuser um nähere Angaben gebeten. Die Auswertung der Antworten ergab, dass alle angefragten Krankenhäuser Patientenarmbänder, jedoch in verschiedenen Varianten, verwenden. Zusammenfassend ist festzustellen, dass gegen die Verwendung von Patientenarmbändern entsprechend den Darstellungen der Kliniken keine datenschutzrechtlichen Bedenken bestehen.

So wird als Rechtsgrundlage zur Verwendung der Patientenarmbänder die Einverständniserklärung der Betroffenen eingeholt. Die Patienten werden entsprechend informiert. Als Zweck ist ausschließlich die Patientenidentifikation definiert. Farbliche Unterscheidungen der Patientenarmbänder, z. B. für organisatorische Zwecke, erfolgen nicht. Die auf den Patientenarmbändern gespeicherten und von außen sichtbaren Daten sind festgelegt und erscheinen für eine Patientenidentifikation erforderlich (meist Name, Vorname, Geburtsdatum, Fallnummer). Die Herstellung der Patientenarmbänder erfolgt in den Kliniken bei der Aufnahme des Patienten. Die Vernichtung der Armbänder erfolgt datenschutzkonform.

11.1.9 Landeskrebsregister Sachsen-Anhalt

Krebs ist in Deutschland inzwischen die zweithäufigste Todesursache. Im Rahmen des Nationalen Krebsplans ist vorgesehen, die Früherkennung, die onkologischen Versorgungsstrukturen und die Qualitätssicherung sowie die Patientenorientierung zu stärken und weiter voranzubringen. Über die Beratungen des Landesbeauftragten zu einem geplanten klinischen Landeskrebsregister wurde im XI. Tätigkeitsbericht (Nr. 10.1.4) berichtet. Infolge der Neuregelung in § 65c SGB V durch das Krebsfrüherkennungs- und -registergesetz (KFRG) mit Vorgaben für die Länder zur Schaffung klinischer Krebsregister ergibt sich die Notwendigkeit landesgesetzlicher Ausgestaltung (vgl. auch **Anlage 18**).

§ 65c SGB V gibt für die klinischen Krebsregister die flächendeckende und vollständige Dokumentation eines bundesweit einheitlichen umfassenden Satzes von klinischen Daten von Krebserkrankungen vor. Die Register sollen die Daten auswerten und die Ergebnisse an die Leistungserbringer rückmelden. Unter anderem sollen weiter die interdisziplinäre, direkt patientenbezogene Zusammenarbeit bei der Behandlung, eine Zusammenarbeit mit Zentren für Onkologie, die Bereitstellung von Daten für die epidemiologischen Krebsregister und die Beteiligung an einrichtungs- und sektorübergreifender Qualitätssicherung bewirkt werden. Finanzielle Grundlage ist im Wesentlichen die Finanzierung durch die Krankenversicherungen in Form von Pauschalen auf der Basis von Meldungen der behandelnden Leistungserbringer, die einmalig für jede verarbeitete Meldung eine Meldevergütung erhalten.

Die Ausgestaltung der Vorgaben führt zu vielen datenschutzrechtlichen Fragen, die mit dem zuständigen Ministerium für Arbeit und Soziales und den Vertretern der drei klinischen Register, aber auch länderübergreifend mit anderen Landesdatenschutzbeauftragten erörtert werden. Dies betrifft u. a. die Abrechnungsmodalitäten mit den Krankenkassen, die Ausgestaltung des Meldedatenabgleichs, die Verwendung von Klardaten oder Pseudonymen und personenbezogene Speicherfristen im dreistelligen Bereich. Anders als bisher soll die Meldung der Leistungserbringer nicht mehr auf der Basis der Einwilligung, sondern gesetzlich verpflichtend erfolgen. Angesichts der Dimensionen und der Bedeutung des Projektes erscheint eine derartige gesetzliche Ausgestaltung zumindest vertretbar. Allerdings wurde darauf gedrungen, die Patienten aufzuklären und ihnen gesetzlich ein Widerspruchsrecht einzuräumen. Ein nicht unkritischer Eingriff in die Patientenhoheit ist die vorgesehene gesetzliche Vorgabe, dass die Register auch die Daten bisheriger Patienten im nunmehrigen Umfang verwenden können, obwohl sie ihnen lediglich auf Basis alter Einwilligungen zur Verfügung stehen und die Widerspruchsmöglichkeit fehlt. Ein weiterer Schwerpunkt ist die Organisation der Datenverwaltung. So besteht der Wunsch, einerseits eine

Vollständigkeit der Daten in allen Bereichen zu erhalten und andererseits Doubletten in der Bewertung zu verhindern. Auch ist eine Anpassung an die Regelungen zum epidemiologischen Gemeinsamen Krebsregister in Berlin erforderlich, da über dieses Register Informationen über Wohnortwechsel und Daten aus den Todesbescheinigungen eingeholt werden und an dieses Register Meldungen erfolgen sollen. Der Landesbeauftragte wird die Umsetzung des KFRG weiter begleiten, die in Form eines Landesgesetzes in der 7. Legislaturperiode erfolgen soll.

11.1.10 Datenübermittlung bei ärztlicher Schweigepflicht

Eine schwangere Patientin wandte sich an den Landesbeauftragten, weil ohne deren Schweigepflichtentbindung ein ärztliches Gutachten eines Neurologen einer Klinik an den überweisenden Arzt, den Hausarzt und zwei andere gynäkologische Kliniken übermittelt wurden. Von ersterer Klinik wurde bestätigt, dass keine schriftliche Schweigepflichtentbindung eingeholt wurde und aufgrund des Zusammenhangs zwischen der Schwangerschaft und der Erkrankung von einer konkludenten Einwilligung ausgegangen worden sei.

Die Übersendung von Arztbriefen stellt eine Übermittlung personenbezogener Daten besonderer Art an Dritte dar. Als Rechtsgrundlage käme u. U. § 28 Abs. 6 Nr. 1 BDSG in Betracht, wenn die Informationen jeweils dem Schutz lebenswichtiger Interessen der Betroffenen dienten. Die Informationen unterlagen allerdings auch der ärztlichen Schweigepflicht nach § 203 Abs. 1 StGB. Eine Durchbrechung der Schweigepflicht ist ausschließlich bei Vorliegen einer Offenbarungsbefugnis rechtmäßig.

Die Voraussetzungen einer konkludenten Einwilligung und Schweigepflichtentbindung als Offenbarungsbefugnis dürften jedoch gefehlt haben. Eine konkludente Einwilligung setzt schlüssiges oder stillschweigendes Verhalten voraus. Es hätte ein Situation vorliegen müssen, die üblicherweise mit der Krankenhausbehandlung derart verbunden ist, dass die Patientin nach aller Erfahrung damit rechnen musste, sodass es keiner ausdrücklichen Erklärung bedurfte. Hierzu muss der Betroffenen zunächst die Notwendigkeit des Zusammenwirkens verschiedener medizinischer Fachkräfte bekannt gewesen sein. Von einer konkludenten Einwilligung in die Hinzuziehung weiterer Fachärzte kann ausgegangen werden, wenn sich Patienten infolge der Art ihrer Erkrankung der Notwendigkeit einer ressortübergreifenden Behandlung bewusst sind. Betroffen sind in der Regel Mitbehandlungen, wie bei radiologischen oder Laborbefunden. Hier ging es jedoch um eine eigenständige andere Art und Qualität der Behandlung. Es lag kein arbeitsteiliges Zusammenwirken vor, mit dem man sich schon mit der Bitte um Behandlung üblicherweise einverstanden erklärt. Auch wenn der Besuch in der Klinik mit dadurch bedingt war, Informationen über mögliche Auswirkungen auf die Schwangerschaft zu erhalten, ließ dies nicht zwingend den Schluss zu, dass damit die Übersendung jedweden Ergebnisses an den eventuell künftig behandelnden Gynäkologen vorab konsentiert ist. Vielmehr hätte die Patientin deutlich zum Ausdruck gebracht haben müssen, dass sie sich trotz der Sensibilität der Befunde der Möglichkeit der eigenen Entscheidung zur Information anderer Ärzte begibt.

Die Fragwürdigkeit der Datenübermittlung wurde weiter deutlich durch die Information an zwei gynäkologische Kliniken. Die Patientin hatte bis dahin nicht entschieden, wo sie entbinden würde. Die Bedenken galten auch bezüglich der Übermittlung an

den Hausarzt, für die die Klinik auf die „Zweckmäßigkeit“ verwies. Dieser Gedanke wird auch in § 73 SGB V aufgegriffen. In § 73 Abs. 1b Satz 3 SGB V ist jedoch bindend vorgegeben, die Betroffenen zu befragen und deren vorherige schriftliche Einwilligung einzuholen. An die Einholung und Dokumentation der Einwilligung sind also strenge Anforderungen zu stellen. In Fällen, in denen die Einwilligung nicht offensichtlich ist, ist dem Selbstbestimmungsrecht und der Patientenhoheit Vorrang zu gewähren. Dabei war hier zu berücksichtigen, dass nicht dargetan war, warum man die Patientin nicht hätte fragen können. Insgesamt war damit festzustellen, dass das Offenbaren medizinischer Daten der Patientin an die gynäkologischen Kliniken und den Hausarzt ohne rechtmäßige Offenbarungsbefugnis erfolgte. Die Klinik sicherte zu, künftig Patientendaten ausschließlich auf nachvollziehbarer rechtmäßiger Grundlage an Dritte zu übermitteln.

11.1.11 Organisation der Arztpraxis

Im Gesundheitswesen werden auch zahlreiche nicht-öffentliche Stellen tätig; das sind insbesondere die freiberuflich tätigen und privatrechtlich organisierten Leistungserbringer, wie etwa die niedergelassenen Ärzte, Zusammenschlüsse von Ärzten oder private Krankenhäuser. Den Schutz der überaus sensiblen Gesundheitsdaten gewährleistet hier der Umstand, dass sie zu den besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG gehören, für die das BDSG an verschiedenen Stellen ein besonders hohes Schutzniveau vorsieht. Zusätzlich bestehen zahlreiche spezialgesetzliche Regelungen. Sie alle korrespondieren mit der ärztlichen Schweigepflicht, die in den Berufsordnungen der Ärzte (vgl. § 9 der Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, § 7 der Musterberufsordnung der Bundeszahnärztekammer) definiert und deren Missachtung durch § 203 StGB unter Strafe gestellt ist.

Zu diesem Themenkomplex erreichten den Landesbeauftragten im Berichtszeitraum Anfragen und Eingaben, die sich auf die Vertraulichkeit in Arztpraxen bezogen. Dabei schilderten einige der Petenten das Problem nur allgemein und bezogen sich nicht auf konkrete Arztpraxen, um das Vertrauensverhältnis zu den behandelnden Ärzten nicht zu gefährden. Es ist daher anzunehmen, dass weitere Betroffene sich aus demselben Grund erst gar nicht an den Landesbeauftragten wenden und die Problematik in einem deutlich höheren Umfang besteht.

Eine datenschutzgerechte bauliche bzw. räumliche Organisation einer Arztpraxis sollte den Empfangsbereich, den Wartebereich und die Behandlungsräume jeweils voneinander bestenfalls durch Wände und Türen abtrennen, die stets geschlossen zu halten sind, wenn für Dritte hörbar über personenbezogene Daten gesprochen wird. Sind die baulichen Voraussetzungen nicht vorhanden und können sie auch nicht nachträglich geschaffen werden, muss zumindest durch geeignete optische und akustische Abschirmungen der bestmögliche Schutz hergestellt werden (z. B. Sitzmöglichkeiten nicht in Hörweite zur Anmeldung, Hintergrundmusik im Wartebereich, Diskretionszone im Anmeldebereich).

Die Behandlungsräume, die für die vertraulichen Gespräche zwischen Arzt und Patient vorgesehen sind, sind stets geschlossen zu halten. Hier genügt es nicht, nur einen Raumteiler oder Vorhang zu installieren, sodass sich in einem Raum mehrere

Patienten aufhalten können, um gleichzeitig z. B. mit dem Arzt zu sprechen oder von der Schwester versorgt zu werden.

In diesem Kontext war eine Eingabe zu bewerten, die eine Arztpraxis in einem medizinischen Versorgungszentrum (MVZ) betraf. Einem Patienten war aufgefallen, dass aufgrund der baulichen Gegebenheiten die vertrauliche Kommunikation zwischen dem Arzt und seinen Patienten von anderen Patienten mitgehört werden kann. Auf Hinweis und Anfrage des Landesbeauftragten und auch des Petenten selbst ergriff der Betreiber des MVZ umgehend umfangreiche Maßnahmen. Er richtete eine Diskretionszone vor dem Empfangstresen ein, entfernte die Sitzmöglichkeiten für wartende Patienten direkt vor einem Untersuchungsraum und erwirkte, dass der Eigentümer der angemieteten Praxisräume die vorhandenen Türen zu den Behandlungs- und Untersuchungsräumen gegen Türen mit einer höheren Schallschutzklasse austauscht. Der Betreiber versicherte, dass die bereits vorhandene Tür zwischen dem Anmelde- und dem Wartebereich stets geschlossen sei und ausreichend gegen Mithören schütze. Ferner wurde das Praxispersonal erneut auf die Anforderungen des Datenschutzes sensibilisiert. Der Landesbeauftragte begrüßt, dass das medizinische Versorgungszentrum die Belange des Datenschutzes sehr ernst nimmt.

In einer Arztpraxis ist ferner die Gesprächsführung an der Anmeldung so zu gestalten, dass Patienten nicht gezwungen sind, medizinische Sachverhalte mündlich vor Unbeteiligten zu offenbaren. Sofern Informationen vor dem Arztgespräch erforderlich sind, hilft unter Umständen ein Fragebogensystem zur schriftlichen Mitteilung.

Sollen medizinische Sachverhalte telefonisch besprochen werden, ist zunächst sicherzustellen, dass der Gesprächspartner wirklich der Patient ist, ggf. durch Abgleich von persönlichen Daten. Diese sind sorgfältig auszuwählen, denn auch gegenüber z. B. Angehörigen, denen etwa das Geburtsdatum in der Regel bekannt sein wird, ist der Arzt nicht von seiner Schweigepflicht entbunden. Zudem ist dafür Sorge zu tragen, dass während des Telefonates Zuhörer nicht aus dem für sie vernehmbaren Gesprächsteil auf die Person des Gesprächspartners schließen können. Erforderlichenfalls sind besonders sensible Gespräche auf ein Telefon in einem geschlossenen Raum umzustellen.

Der Landesbeauftragte warnt auch davor, Patientenunterlagen für andere Patienten sichtbar, z. B. im Empfangsbereich oder im Behandlungsraum, abzulegen. Die Karteikarten, die dem Arzt den nächsten Patienten in der Reihenfolge anzeigen, oder die Rezepte und Bescheinigungen, die auf die Unterschrift des Arztes warten, sind vor den Blicken Dritter zu schützen. Dies gilt auch für PC-Bildschirme und Faxgeräte, wenn sich darin lesbar Ausdrucke befinden können.

Die neuen technischen Möglichkeiten machen auch vor Arztpraxen nicht halt. Sie eröffnen stetig neue Fragestellungen, etwa bei der Kommunikation per Fax und E-Mail, im Hinblick auf Praxisverwaltungssysteme oder die Vernetzung innerhalb der Praxis und mit Externen. Auch die Anwendungsbereiche der Telemedizin werden sich im Interesse einer besseren Versorgungslage insbesondere in ländlichen Räumen oder in speziellen Fachbereichen der Medizin ausweiten. Zu beachten ist dabei insbesondere, dass Daten sicher gegen unbefugte Zugriffe zu schützen sind, etwa durch Zugriffsberechtigungskonzepte und Vergabe sicherer Passwörter, Verschlüsselung von E-Mails und Backupmedien. Vor jeglichem Technikeinsatz in der Arztpra-

xis ist stets eine eingehende Prüfung auf Aspekte des Datenschutzes und der Datensicherheit, ggf. mit Beratung durch den Landesbeauftragten, angezeigt.

Die Auftragsdatenverarbeitung im Gesundheitswesen befindet sich derzeit rechtlich noch in einem Graubereich. Es ist ganz und gar nicht unüblich, dass sich insbesondere niedergelassene Ärztinnen und Ärzte für die Pflege und Wartung ihres IT-Systems eines externen Dienstleisters bedienen. Allerdings dürfen sie dem Dienstleister dabei nach der aktuellen Rechtslage keinen Zugang zu Patientendaten gewähren, es sei denn die Patienten hätten sich hiermit ausdrücklich und freiwillig einverstanden erklärt, was in der Praxis kaum umzusetzen ist (zur Frage der wirksamen Einwilligung zur Verarbeitung von Gesundheitsdaten vgl. Nr. 10.1.5 des XI. Tätigkeitsberichts). Beachten Ärzte diese Trennung nicht, würden sie ihre ärztliche Schweigepflicht verletzen und sich nach § 203 StGB strafbar machen (vgl. hierzu etwa das Urteil des Landgerichts Flensburg vom 5. Juli 2013, Az. 4 O 54/11, ZMGR 2013, 434). Die Absicherung von Patientendaten gegenüber jemandem, der ein IT-System betreut und dafür in der Regel Administrationsrechte benötigt, dürfte jedoch in der Praxis äußerst schwierig sein und wiederum Spezialwissen erfordern. Aus diesem Grund dürfte das Outsourcing von IT-Leistungen in der Arztpraxis derzeit in der Regel als unzulässig zu bewerten sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich dieser Problematik bereits vielfach angenommen. Auch dies führte zu der Entschließung der Datenschutzkonferenz vom 1. und 2. Oktober 2013 (**Anlage 4**), mit der angemessene datenschutzgerechte gesetzliche Regelungen für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, gefordert wurden.

Das sogenannte eHealth-Gesetz rückt das Thema erneut in den Fokus. Die Datenschutzkonferenz hat am 18. und 19. März 2015 die Forderung daher erneuert und konkretisiert (**Anlage 24**; vgl. Nr. 11.1.3).

Aus Anlass einer entsprechenden Anfrage im Berichtszeitraum stellte der Landesbeauftragte klar, dass auch in einer Arztpraxis ein betrieblicher Beauftragter für den Datenschutz zu bestellen ist, wenn das Unternehmen in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt; bei der nicht-automatisierten Verarbeitung sind es mindestens 20 Personen. Der betriebliche Datenschutzbeauftragte muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen und wirkt auf die Einhaltung der Datenschutzvorschriften hin (§§ 4f Abs. 1 und 2, 4g Abs. 1 BDSG).

Die hier dargestellten Aspekte des Umganges mit personenbezogenen Daten in einer Arztpraxis stellen nur eine Auswahl dar. Einen vertiefenden Blick bietet die Initiative „Mit Sicherheit gut behandelt“ des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz gemeinsam mit der Kassenärztlichen Vereinigung Rheinland-Pfalz. Die Initiative betreibt eine Homepage[9], bietet Fortbildungen und Vorträge auf regionalen Veranstaltungen an, deren Material zum Teil online abrufbar ist, und veröffentlicht in Printmedien. Auch die Bundesärztekammer und die Kassenärztliche Bundesvereinigung haben ihre Empfehlungen zur ärztlichen

[9] http://www.mit-sicherheit-gut-behandelt.de

Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis im Mai 2014 in einer aktualisierten Fassung veröffentlicht. Zudem liegen datenschutzrechtliche Leitfäden im Hinblick auf die Hard- und Software in Arztpraxen von den ärztlichen und zahnärztlichen Kammern und Vereinigungen auf Bundesebene vor.

Können sich Patienten auf den vertraulichen Umgang mit ihren Daten verlassen, stellt dies für sie neben der ärztlichen Fachkompetenz zweifelsohne auch ein wesentliches Qualitätsmerkmal einer Arztpraxis dar. Das Einhalten datenschutzrechtlicher Anforderungen sollte für Ärztinnen und Ärzte aus diesem Grund ein wichtiges Anliegen sein. Die Sensibilisierung des gesamten Praxispersonals ist hierfür Grundvoraussetzung.

11.1.12 Herzinfarktregister Sachsen-Anhalt

Im XI. Tätigkeitsbericht (Nr. 10.1.5) wurde die umfängliche Beratung des Projektes Regionales Herzinfarktregister Sachsen-Anhalt (RHESA) dargestellt. Für die notwendige Einbeziehung von verschiedenen Stellen (u. a. Gesundheitsamt, Krankenhaus, Hausarzt, Rettungsdienst) und in Abhängigkeit vom Vorliegen bzw. Nichtvorliegen einer Einwilligung wurden datenschutzkonforme Lösungen gesucht. Die Beratungen wurden im Berichtszeitraum abgeschlossen. Das RHESA hat ein umfassendes Datenschutzkonzept erstellt und seine Arbeit danach aufgenommen.

Nach einigen Monaten hat der Landesbeauftragte das RHESA an der Medizinischen Fakultät der Martin-Luther-Universität Halle-Wittenberg besucht und sich über das datenschutzkonforme Verfahren informiert. Im Vordergrund standen die Wege und Verfahren, die die Anonymisierung von Informationen zu Personen sicherstellen sollen, deren Einverständnis in die Datenverarbeitung nicht vorliegt. So sollen z. B. bei nicht überlebten Infarkten die Gesundheitsämter eine Kopie der Todesbescheinigung an das RHESA senden, auf der die personenidentifizierenden Daten geschwärzt sind. Der auf der Todesbescheinigung dokumentierte zuletzt behandelnde Arzt erhält ein Anschreiben des Gesundheitsamtes, einen Erhebungsbogen und einen an das RHESA adressierten, frankierten Umschlag. Auf dem Erhebungsbogen soll vom Gesundheitsamt als Pseudonym u. a. die Sterbebuchnummer eingetragen sein. Der Arzt kann dann den Erhebungsbogen ohne identifizierende Angaben in dem Umschlag an das RHESA senden. Eine Datenzusammenführung wird ohne Identifikation über das Pseudonym möglich. Auch Einsatzprotokolle der Rettungsdienste werden vom RHESA anhand der durch die ärztlichen Erhebungsbögen bekannten Einsatz-Nummer angefordert. Die Rettungsdienste sind aufgefordert, die identifizierenden Daten durch Schwärzen und Kopieren der Schwärzungen unkenntlich zu machen. Eine Zuordnung ist über die Einsatz-Nummer möglich.

Der Landesbeauftragte konnte vor Ort feststellen, dass die im Datenschutzkonzept vorgesehenen Verfahren eingehalten werden. Lediglich bei einzelnen Schwärzungen der Gesundheitsämter war das nochmalige Kopieren der Schwärzung unterlassen worden. Die Namen der Betroffenen waren bei entsprechender Beleuchtung noch erkennbar. Insoweit wurde Abhilfe gefordert und durch das RHESA zugesagt. Im Rahmen der Beratung konnten einige weitere Hinweise und Empfehlungen, z. B. zur Sicherung der Schriftgutentsorgung und zur Einschränkung administrativer Rechte auf den Datenbanken gegeben werden, deren Berücksichtigung ebenfalls zugesagt wurde.

11.1.13 Maßregelvollzug

Im XI. Tätigkeitsbericht (Nr. 10.1.3.) wurden der Informationsbesuch im Landeskrankenhaus in Uchtspringe und einige sich daraus ergebende datenschutzrechtliche Empfehlungen beschrieben. Das Landeskrankenhaus hat inzwischen ausführlich Stellung genommen. So wurde z. B. die Videoüberwachung im Foyer mit Hinweis auf die verschiedenen Nutzungsbedingungen und beteiligten Personengruppen nachvollziehbar begründet. Die Maßgaben zu optisch-elektronischen Beobachtungen und Aufzeichnungen in Einzelzimmern wurden dagegen aufgenommen und Beschränkungen eingeführt. Zur Überbrückung bediente man sich der Möglichkeit, die Kameras zuzukleben, um unbeobachtete Nutzungen der Räume zu ermöglichen. Auch die Hinweise zum Zugriff durch Pflegekräfte auf Präsenzakten führten zur Änderung der Verfahrensweisen.

Im IX. Tätigkeitsbericht (Nr. 12.3) und im X. Tätigkeitsbericht (Nr. 12.4) hatte der Landesbeauftragte ausführlich die Begleitung der Novellierung des Maßregelvollzugsrechts dargestellt. Im Nachgang entstand eine Diskussion unter Beteiligung des Ministeriums für Arbeit und Soziales und des Landeshauptarchivs über die Frage, ob Unterlagen aus dem Maßregelvollzug dem Archiv anzubieten sind. Seitens des Ministeriums wurde auf die Löschungsvorgabe des § 37 MVollzG LSA und die besondere Sensibilität der Akten zur Unterbringung hingewiesen. Der Landesbeauftragte stimmte jedoch nach ausführlicher Erörterung und Prüfung der Auffassung des Landeshauptarchivs zu. Ein Löschungsgebot schließt keine Anbietung an das zuständige Archiv auf archivgesetzlicher Grundlage aus. Die Archivierung erfolgt auf neuer gesetzlicher Grundlage im Anschluss an das Löschungsgebot (siehe dazu auch Nr. 10.1).

11.1.14 Spenderfragebogen im Blutspendedienst

Ein potentieller Blutspender bat den Landesbeauftragten um datenschutzrechtliche Prüfung eines neuen Spenderfragebogens, der im Rahmen eines Blutspendetermins vorgelegt wurde und sehr intime Fragen zum Sexualverhalten des Spenders enthielt. Außerdem war festzustellen, dass sich die Einverständniserklärung des Spenders nicht nur auf die Speicherung der spenderrelevenaten Daten bezog, sondern gleichzeitig auf die Verwendung des sonst zu vernichtenden Blutes für verschiedene Zwecke außerhalb des Blutspendezwecks, z. B. auch für Forschungs- und Entwicklungsvorhaben der Klinik und mit ihr zusammenarbeitender Institutionen. Der Fragebogen orientierte sich an der bundeseinheitlichen Vorlage des Paul-Ehrlich-Institutes und wurde von Vertretern der Deutschen Gesellschaft für Transfusionsmedizin und Immunhämatologie und dem Berufsverband der Deutschen Transfusionsmediziner entwickelt.

Nach § 11 i. V. m. § 5 Abs. 1 Transfusionsgesetz (TFG) dürfen Spendeeinrichtungen personenbezogene Daten spendewilliger und spendender Personen erheben, verarbeiten und nutzen, soweit dies nach dem Stand der medizinischen Wissenschaft und Technik für eine erforderliche Auswahl der Spender bzw. einen Ausschluss oder eine Zurückstellung einzelner Personen aus Gründen der Risikovermeidung erforderlich ist. Aufgrund der gem. § 12a TFG erlassenen Richtlinien der Bundesärztekammer sind auch die Fragen zum ungeschützten und geschützten Intimkontakt grundsätzlich erforderlich, um eine Risikogruppenzugehörigkeit (heterosexuelle Personen mit se-

xuellem Risikoverhalten, z. B. Geschlechtsverkehr mit häufig wechselnden Partnern, Männer mit Sexualverkehr mit Männern und männliche oder weibliche Prostituierte) zu ermitteln. Die Kenntnis, zu welcher konkreten Risikogruppe der Spendewillige gehört, ist jedoch nicht erforderlich, da bei allen Risikogruppen gleichermaßen ein Ausschluss von der Spende erfolgt. Der Landesbeauftragte konnte daher eine Änderung des Fragebogens insoweit erreichen, dass diese Fragen in einem gemeinsamen Fragenkomplex zusammengefasst sind. Muss nun eine der Fragen mit ja beantwortet werden, hat der Spender die Wahl, den gesamten Fragenkomplex mit ja zu beantworten (ohne das konkrete Risiko preiszugeben) oder die Frage unbeantwortet zu lassen und die Spende zu beenden. Die Einverständniserklärung wurde nunmehr zweigeteilt in das Einverständnis zur eigentlichen Spende und für die Verwendung der Blutreste für interne Zwecke. Hierzu wird zur Information des Spenders ein Infoblatt ausgelegt, in dem die einzelnen Verwendungszwecke erläutert werden. Auf das ausliegende Informationsblatt wird im Text der Einverständniserklärung ausdrücklich verwiesen. Aufgrund dieser Anpassungen bestehen nun keine datenschutzrechtlichen Bedenken mehr.

11.1.15 Verordnungen zum Wohn- und Teilhabegesetz

Wie bereits im X. Tätigkeitsbericht (Nr. 22.17) dargestellt, hat der Gesetzgeber beim Entwurf des Wohn- und Teilhabegesetzes (WTG LSA) den Landesbeauftragten frühzeitig beteiligt. Im Berichtszeitraum legte das zuständige Ministerium dem Landesbeauftragten den Entwurf einer Mitwirkungsverordnung zum WTG LSA und den Entwurf einer Personalverordnung zum WTG LSA zur Anhörung vor.

Mitwirkungsverordnung

Der Entwurf der WTG-MitwVO sah zunächst vor, dass der Träger der zuständigen Behörde Angaben zum Zeitpunkt der Wahl einer Bewohnervertretung, zum Wahlergebnis und zur Anzahl der Mitglieder der Bewohnervertretung mitteilt. Der Landesbeauftragte wies darauf hin, dass die Formulierung „Wahlergebnis“ zu unbestimmt sei und dadurch nicht deutlich ist, ob die Zahl der Wähler, eine namentliche Aufstellung der Gewählten, der jeweilige Stimmenanteil oder die Stimmenverteilung zu melden sind. Das Ministerium für Arbeit und Soziales teilte mit, dass durch die namentliche Meldung der Gewählten der Heimaufsichtsbehörde ermöglicht werden soll, die Mitwirkungsgremien anzuschreiben und zu beraten. Bei datenschutzrechtlichen Bedenken sei jedoch auch eine Variante ohne Nennung der Namen denkbar; dann könnten die Vertretungen nicht persönlich angesprochen werden. Der Landesbeauftragte stellte dazu in Frage, ob für die Unterrichtung der Bewohnervertretungen über die Wahl und die Aufgaben und Rechte der Bewohnervertretung die Vorhaltung der Daten sämtlicher Mitglieder dieser Mitwirkungsgremien erforderlich ist. Angesichts der Zahl der stationären Einrichtungen und sonstigen nicht selbstorganisierten Wohnformen dürfte der Aufwand, die Daten von geschätzt weit mehr als 1.000 Mitgliedern der Bewohnervertretungen vorzuhalten und ständig aktuell zu halten, nicht unerheblich sein. Zudem kommen allgemeine Beratungen z. B. auf dem Schriftweg durch Zurverfügungstellen von Faltblättern oder hinweisenden Schreiben in Betracht, wofür die namentliche Kenntnis der Mitglieder nicht erforderlich ist. Es dürfte ausreichen, die Vertretungen nicht persönlich anzusprechen. Das Ministerium hielt die Argumente für überzeugend und kündigte an, die Formulierung im Verordnungsentwurf zu ändern.

Entgegen der Empfehlung des Landesbeauftragten hat das Ministerium im Einvernehmen mit dem Landtag die Formulierung „das Wahlergebnis“ beibehalten (§ 6 WTG-MitwVO, GVBl. LSA 2016 S. 14, 16).

Personalverordnung

§ 33 Abs. 1 Satz 1 Nr. 2 WTG LSA ermächtigt das für das Heimrecht zuständige Ministerium, durch Verordnung Regelungen u. a. für die Eignung der Leitungskräfte und der Beschäftigten in stationären Einrichtungen und betreuten Wohngruppen zu erlassen. Der Entwurf der Personalverordnung zum WTG LSA sah vor, dass vor der Einstellung der Leitungskräfte der zuständigen Behörde zum Nachweis der persönlichen Eignung und bei begründeten Zweifeln an der persönlichen Eignung ein Führungszeugnis nach § 30 Abs. 5 BZRG vorzulegen ist. Nach § 12 WTG LSA muss der Betreiber einer stationären Einrichtung der zuständigen Behörde spätestens drei Monate vor der geplanten Inbetriebnahme darlegen, dass er die Anforderungen nach § 11 Abs. 1 bis 4 WTG LSA erfüllt. Nach § 11 Abs. 4 WTG LSA hat der Träger sicherzustellen, dass die persönliche und fachliche Eignung der Beschäftigten für die von ihnen zu leistende Tätigkeit ausreicht. Dazu hat der Betreiber Angaben zum Personal zu machen; die zuständige Behörde kann weitere Angaben verlangen (§ 12 Abs. 2 Satz 1 WTG LSA). Gegen die Vorlage eines Führungszeugnisses für Leitungskräfte bei der zuständigen Behörde bestanden wegen der Befugnisse im WTG LSA keine Bedenken.

Bei betreuten Wohngruppen nach § 4 Abs. 3 WTG LSA (Wohngruppen für Menschen mit Behinderungen) sollte nach § 6 Abs. 1 i. V. m. § 3 Abs. 2 WTG-PersVO für die Leitungskräfte der zuständigen Behörde ebenfalls ein Führungszeugnis vorzulegen sein. Die Anforderungen an die persönliche Eignung der Beschäftigten ergeben sich nach § 11 Abs. 4 i. V. m. § 12 Abs. 2 WTG LSA. Diese Regelungen beziehen sich jedoch ausschließlich auf stationäre Einrichtungen und sind deshalb mangels Verweis nicht auf sonstige nicht selbst organisierte Wohnformen anwendbar. Die Anforderung eines Führungszeugnisses von Leitungskräften betreuter Wohngruppen zur Vorlage bei der zuständigen Behörde erschien bedenklich, worauf der Landesbeauftragte hingewiesen hat. Ob dies beim Beschluss der Verordnung berücksichtigt wird, bleibt abzuwarten.

11.1.16 Dopingbekämpfung

Im XI. Tätigkeitsbericht (Nr. 10.1.14) hatte der Landesbeauftragte für die Bekämpfung des Dopings datenschutzrechtliche Regelungen angemahnt, die sicherstellen, dass durch die notwendigen Kontrollen die Menschenwürde der Sportler nicht beeinträchtigt und der Athlet nicht zum gläsernen Sportler herabgewürdigt wird.

Im Berichtszeitraum haben die Bundesministerien der Justiz und für Verbraucherschutz, des Innern und für Gesundheit den Entwurf eines „Gesetzes gegen Doping im Sport“ (Anti-Doping-Gesetz – AntiDopG, BR-Drs 126/15) vorgelegt, zu dem die Datenschutzbeauftragten der Länder Rheinland-Pfalz und Schleswig-Holstein eine Stellungnahme erarbeitet haben, der sich der Landesbeauftragte angeschlossen hat. Leider wurde die Stellungnahme im Gesetz vom 10. Dezember 2015 (BGBl. I S. 2210) nicht berücksichtigt.

Von den Datenschutzaufsichtsbehörden wird allgemein anerkannt, dass ein globales System der Dopingbekämpfung bei internationalen Sportveranstaltungen notwendig ist. Die Dopingbekämpfung muss aber die Menschenrechte auf Privatheit und Wahrung der Intimsphäre sowie auf Schutz der persönlichen Daten der Sportler angemessen beachten. Die vormalige rechtliche Legitimation für die Datenverarbeitung erfolgte über Einwilligungen der Sportler. Diese Einwilligungen genügten jedoch weder den nationalen noch den europäischen datenschutzrechtlichen Anforderungen. Sie wurden nicht freiwillig erteilt, waren zu unbestimmt und erlaubten zum Teil unverhältnismäßige Eingriffe in das Recht auf informationelle Selbstbestimmung. Insofern wird grundsätzlich begrüßt, dass die Datenverarbeitungen auf eine gesetzliche Grundlage gestellt wurden.

Allerdings ist der Datenschutz in dem Gesetz nur unzureichend berücksichtigt. Es bestehen Zweifel daran, dass es den verfassungsrechtlichen Anforderungen des Wesentlichkeitsgrundsatzes und der Normbestimmtheit sowie den bestehenden staatlichen Schutzpflichten zugunsten der Athleten gerecht wird.

So ist die NADA nach § 9 des AntiDopG berechtigt, zur „Durchführung ihres Dopingkontrollsystems“ bestimmte personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Durch die pauschale Bezugnahme auf das Dopingkontrollsystem der NADA entledigt sich der Gesetzgeber seiner Aufgabe, selbst einen Ausgleich der widerstreitenden einschlägigen Interessen – dem Interesse an einem fairen und gesundheitlich verantwortbaren Wettkampfsport einerseits und dem Interesse der Sportlerinnen und Sportler an der freien Ausübung ihres Berufs sowie an der Wahrung ihrer Privat- und Intimsphäre andererseits – zu finden. Es fehlen Beschreibungen, was unter einem Dopingkontrollsystem zu verstehen ist, z. B. zur Auswahl der Athleten im Rahmen von Trainingskontrollen und zu den Meldepflichten der Athleten. Durch fehlende Konkretisierungen im Gesetz werden die Einzelheiten in die Regelungskompetenz einer privaten Stiftung verlagert.

Problematisch können auch die nach § 10 Abs. 2 AntiDopG vorgesehenen Übermittlungen personenbezogener Daten (auch Gesundheitsdaten!) an internationale Sportfachverbände, Veranstalter von Sportwettkämpfen sowie die WADA sein. Gesundheitsbezogene Daten unterliegen nach § 3 Abs. 9 BDSG einem besonderen Schutz. Bei beabsichtigten Übermittlungen in das außereuropäische Ausland muss sichergestellt werden, dass diese nur erfolgen, wenn die Ausnahmen des § 4c Abs. 1 BDSG vorliegen oder die NADA ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Greifen die Ausnahmen nicht und liegen keine Garantien vor, müssen die Übermittlungen unterbleiben.

Der Landtag unterstützte das Gesetzesanliegen, ohne allerdings Verbesserungen beim Datenschutz anzumahnen (LT-Drs. 6/4237).

11.2 Sozialwesen

11.2.1 Kontoauszüge in SGB II-Verfahren

Immer wieder erhält der Landesbeauftragte Anfragen besorgter Kunden von kommunalen Trägern nach dem SGB II (Jobcenter der Optionskommunen) zur Zulässigkeit

der Anforderung von Kontoauszügen. Dies wurde bereits im XI. Tätigkeitsbericht (Nr. 10.2.1) unter Bezugnahme auf frühere Berichte und die Hinweise von Landesbeauftragten zur datenschutzgerechten Anforderung von Kontoauszügen erwähnt.

Eine Eingabe erläuterte, dass es nach der Rechtsprechung eines Gerichts doch unzulässig sei, Kontoauszüge zu vergangenen Monaten zu erfragen. Dem steht jedoch eine Entscheidung des Bundessozialgerichts (19. September 2008, B 14 AS 45/07 R, juris) entgegen, wonach die grundsätzliche Verpflichtung besteht, die Kontoauszüge der letzten drei Monate vorzulegen. Allerdings wird datenschutzkonform betont, dass die Empfänger von Zahlungen geschwärzt werden können, wenn andernfalls besondere personenbezogene Daten (Parteizugehörigkeit, konfessionelles Bekenntnis etc.) offengelegt werden müssten.

Weiter wird auch häufig die Frage angesprochen, ob denn die erhobenen Informationen in den Akten gespeichert werden dürfen. Dies hängt von der Erforderlichkeit ab. Sind die Informationen für die Berechnung, eventuelle Nachberechnungen oder andere Arbeitsschritte im Rahmen der Leistungsgewährung einschließlich Rechnungsprüfung notwendig, ist die Erforderlichkeit gegeben (hierzu sehr weitreichend Bayerisches Landessozialgericht vom 14. November 2013, Az. L 7 AS 579/13 B ER, juris). Nicht erforderlich ist die Speicherung zum Beispiel, wenn die Auszüge nur abermals bei Folgeanträgen dokumentieren, dass keine Einkünfte vorhanden sind. Hier reicht auch für künftige Berechnungen die Feststellung durch Sichtvermerk, dass sich nichts geändert hat.

Ein Jobcenter, das Akten digital führt, hat mitgeteilt, dass auch die Kontoauszüge zunächst generell eingescannt werden. Dies sei zulässig, da kein Speichern vorliege. Schließlich diene das Einscannen und digitale Ablegen nur dazu, den Sachbearbeitern die Daten nach der Aufnahme für die Bearbeitung der Anträge für drei Wochen zur Verfügung zu stellen. Werden die Daten nicht aufgegriffen und in den Vorgang kopiert, würden sie nach drei Wochen gelöscht. Auch das kurzzeitige „Zwischenspeichern“ für die Bearbeitung ist ein datenschutzrelevanter Vorgang und damit nur zulässig, wenn es für die Aufgabenerfüllung erforderlich ist, § 67c Abs. 1 Satz 1 SGB X. Es erschien jedoch nachvollziehbar, dass direkt bei der Aufnahme des Antrags nicht immer eine abschließende Bearbeitung möglich ist, sodass nach Ende des Publikumsverkehrs eine detaillierte Prüfung der Anträge erfolgt. In diesem Rahmen ist zu würdigen, ob die Angaben für spätere Berechnungen in den Vorgang übernommen werden oder ob ein Sichtvermerk ausreicht. Die materielle Prüfung, ob relevante Daten in den Kontoauszügen enthalten sind, ist ggf. sehr aufwändig. Zur Steigerung der Effizienz der Antragsbearbeitung und zur Verkürzung der Erörterungen mit Antragstellerinnen und Antragstellern entwickelte das Jobcenter im Kundeninteresse dieses Verfahren, das eine inhaltliche Prüfung eingescannter Kontoauszüge gestattet. Sie sind nur den zuständigen Bearbeitern zugänglich, die die Überprüfung, ob die Daten in die Akte übertragen werden müssen, vornehmen.

Das Jobcenter hat in Abstimmung mit dem Landesbeauftragten eine detaillierte Dienstanweisung zur Prüfung von Kontoauszügen erstellt. Für den Fall, dass nur einzelne Informationen aus den Auszügen benötigt werden, wurde hierfür ein Prüfblatt entwickelt, auf dem die Einzeldaten notiert werden können. Die Kunden erhalten ein Merkblatt hierzu. Sie werden auf Schwärzungsmöglichkeiten hingewiesen.

11.2.2 Hausbesuche des Jobcenters

Eine Petentin teilte mit, sie sei im Jobcenter um ein Gespräch gebeten worden. Sie habe jedoch mit dem Hinweis abgelehnt, sie würde lieber schriftlich Stellung nehmen. Daraufhin erhielt sie eine Ankündigung eines Hausbesuchs zur Klärung eines Sachverhalts vor Ort. Mangels näherer Begründung des beabsichtigten Besuchs sagte die Petentin den Besuch ab.

Der Landesbeauftragte teilte der Petentin zunächst mit, dass ihre Mitwirkung bei der Antragstellung nach § 60 Abs. 1 SGB I geboten sei. Nach § 60 Abs. 2 SGB I sind ggf. Vordrucke zu verwenden. Grundsätzlich aber ist das Verwaltungsverfahren nicht an eine bestimmte Form gebunden. § 9 Satz 2 SGB X fordert vielmehr, das Verfahren einfach, zweckmäßig und zügig zu gestalten. Für einfache Nachfragen jenseits der grundsätzlich zu verwendenden sachdienlichen Antragsvordrucke bietet sich daher das mündliche Verfahren an. Im Rahmen der Sachverhaltsermittlung von Amts wegen kann das Jobcenter zur Feststellung von Leistungsvoraussetzungen auch Hausbesuche durchführen. Eine Pflicht, Zutritt zu gewähren, besteht zwar nicht. Sind allerdings die Ermittlungsmaßnahmen legitim, kann die Verweigerung mit Nachteilen verbunden sein. Das Jobcenter wies in einer Stellungnahme hierzu vornehmlich auf die Vorgaben der §§ 20 und 21 SGB X (Untersuchungsgrundsatz, Beweismittel) hin. Man habe zum wiederholten Male eine anonyme Anzeige erhalten, wonach die Petentin einen Partner habe. Bei der Prüfung eheähnlicher Gemeinschaften läge auf der Hand, dass eine inhaltliche Ankündigung vorher nicht erfolgen könne.

Die Auffassung des Jobcenters übersieht leider wie so oft, dass die Verfahrensvorgaben aus den §§ 20, 21 SGB X bei der Erhebung und Verarbeitung von Sozialdaten gegenüber den Vorschriften über den Sozialdatenschutz nachrangig sind (so ausdrücklich § 37 Satz 3 SGB I). Daher stehen insbesondere beim Hausbesuch, der den geschützten Bereich des Art. 13 Abs. 1 GG (Grundrecht auf Unverletzlichkeit der Wohnung) betrifft, der Grundsatz der Verhältnismäßigkeit und die Erforderlichkeit im Vordergrund. Der Landesbeauftragte hat auf die strengen Anforderungen an die Zulässigkeit eines Hausbesuchs hingewiesen, die sich auch in den fachlichen Hinweisen der Bundesagentur für Arbeit auf der dortigen Homepage finden. Sie beruhen auf den auch für das Jobcenter geltenden verfassungsrechtlichen Maßstäben (vgl. auch Nr. 10.2.3 des XI. Tätigkeitsberichtes).

Die Stellungnahmen des Jobcenters machten eine nähere Prüfung und Erörterung in der Behörde nötig. Der Hausbesuch stellt einen der größtmöglichen Grundrechtseingriffe dar, die dem Jobcenter im Rahmen der Amtsermittlung zukommen. Eine vorherige Befragung ist das mit großem Abstand mildere Mittel. Dies war dem Jobcenter zwar bewusst, es gab aber an, eine Befragung sei zur Zweckerreichung nur sehr eingeschränkt geeignet. Im Ergebnis erschien das Vorgehen des Jobcenters nach Würdigung des gesamten Sachverhalts allerdings noch vertretbar. Die Mutmaßung, dass die Befragung der Betroffenen nichts bringe, war dennoch merkwürdig. Schließlich hatte man zunächst selbst das Gespräch gesucht.

Die umfängliche obergerichtliche Rechtsprechung zur Zulässigkeit von Hausbesuchen lässt derartige Maßnahmen zur Klärung von Wohnverhältnissen zu. In den positiv entschiedenen Fällen lagen aber gravierende Anhaltspunkte für die Notwendigkeit einer Prüfung vor Ort vor. Ob allein eine anonyme Anzeige ausreicht, wird dabei offen gelassen. Vielmehr muss die Zweckdienlichkeit definiert sein. Die zu erheben-

den Sachverhalte müssen direkt unter leistungsrelevante Tatbestandsmerkmale zu subsumieren sein (z. B. Überprüfung von behaupteten Beschädigungen der Einrichtung; Prüfung, ob noch Brennmaterial auf dem Grundstück vorhanden ist, um den Antrag auf weiteres Brennmaterial zurückweisen zu können). Insgesamt begegnet die Durchführung von Hausbesuchen zur Erhebung von tatbestandsrelevanten Merkmalen hinsichtlich eheähnlicher Lebensgemeinschaften vielfach Bedenken. Die Erforderlichkeit eines Hausbesuches dürfte in erheblichem Maße zweifelhaft sein, wenn selbst bei sachgerechter Beantwortung der zu stellenden Fragen und zielführender Feststellung der zu untersuchenden Tatsachen letztendlich nicht auf das Vorliegen einer leistungsrelevanten eheähnlichen Lebensgemeinschaft geschlossen werden kann.

Nach der Rechtsprechung setzt die Feststellung einer leistungsrelevanten eheähnlichen Lebensgemeinschaft auch unter Berücksichtigung der Beweiserleichterung hinsichtlich des subjektiven Tatbestandes nach § 7 Abs. 3a SGB II voraus, dass es sich um Partner handeln muss, die einen gemeinsamen Haushalt führen. Eine Partnerschaft zeichnet sich dadurch aus, dass sie auf Ausschließlichkeit und auf eine gewisse Dauer angelegt ist und daneben keine Lebensgemeinschaft gleicher Art und Intensität zulässt. Weiter muss die rechtliche zulässige Möglichkeit einer Heirat bzw. Gründung einer Lebenspartnerschaft bestehen. Das Feststellen des weiteren Merkmals einer Haushaltsgemeinschaft setzt über die gemeinsame Nutzung einer Wohnung wesentliche weitere Umstände voraus, die darauf hindeuten, dass die Beteiligten ihr tägliches Leben aufeinander abgestimmt haben (Einnahme von Mahlzeiten, arbeitsteilige Haushaltsführung, gemeinsame Freizeitgestaltung und Hobbies, „Wirtschaften aus einem Topf“). Auch eine Gemeinschaftskasse ist noch kein Beleg für eine Wirtschaftsgemeinschaft. Vielmehr muss die gemeinsame Haushaltsführung gemeinschaftlich, abhängig von der jeweiligen wirtschaftlichen und körperlichen Leistungsfähigkeit, erfolgen. Wesentliche objektive Tatbestandsmerkmale sind daher nicht durch die Inaugenscheinnahme vor Ort, sondern letztlich nur durch Befragung der Betroffenen zu klären. Eine Inaugenscheinnahme vor Ort dient eher der Beseitigung letzter Zweifel.

Auch die Fragen, die in der hausinternen Handlungsanweisung des Jobcenters für Hausbesuche vorgegeben werden, zeigen, dass tragfähige Schlüsse auf Leistungsmerkmale kaum möglich sind. Die Frage, wie lange man ein Paar sei, lässt den Begriff „Paar“ und damit mögliche Schlussfolgerungen völlig offen. Die Frage nach der Länge des Zusammenwohnens lässt sich ohnehin nur durch Befragung, nicht jedoch durch Inaugenscheinnahme klären. Die Frage nach einem gemeinsamen Briefkasten oder einer gemeinsamen Klingel kann keine relevanten Kenntnisse erbringen, da dies auch typische Merkmale einer Wohngemeinschaft sind. So scheint auch die Frage nach dem Verschließen der Räumlichkeiten irrelevant. Schon bei einfachsten Wohngemeinschaften sind die jeweiligen Räumlichkeiten oft nicht verschlossen. Fragen zu Wohnungsgröße, Anzahl der Räume (Mietvertrag) und Teilung der Nebenkosten sowie zum Eigentum der Wohnungseinrichtung sind ebenso nicht durch Inaugenscheinnahme zu klären, wie die Frage nach der gemeinsamen Erledigung der Hausarbeit, gemeinsamen Einkäufen und deren Finanzierung sowie gemeinsamer Freizeitgestaltung. Auch Fragen zum Sorgerecht für Kinder und dessen Ausübung, zum Empfang von Kindergeld u. ä. Leistungen sowie Unterhaltszahlungen, zu Zugriffen auf das Konto des Anderen und das Bestehen von Lebensversicherungen bzw. finanziellen Verbindlichkeiten sind nicht durch Inaugenscheinnahme vor Ort zu klä-

ren. Insgesamt erscheint daher ein Hausbesuch als gravierender Grundrechtseingriff nur bei Vorliegen vielfältiger weiterer zuvor durch Befragung zu ermittelnder Merkmale verhältnismäßig.

11.2.3 Datenabgleich nach § 52 SGB II

Ein Petent machte den Landesbeauftragten darauf aufmerksam, dass dem zuständigen Jobcenter Kontendetails bekannt sind, die über die nach § 52 SGB II im automatisierten Datenabgleich vorgesehenen Kontenabfragen hinausgehen würden.

Das um Stellungnahme gebetene Jobcenter teilte mit, dass nach § 52 Abs. 1 SGB II die Bundesagentur und die zugelassenen Träger ermächtigt sind, Personen, die Leistungen nach dem SGB II beziehen, im Wege des automatisierten Datenabgleichs zu überprüfen. Dieser Datenabgleich hat sich u. a. darauf zu beziehen, ob und in welchem Umfang Zeiten des Leistungsbezugs nach dem SGB II mit Zeiten einer Versicherungspflicht oder Zeiten einer geringfügigen Beschäftigung zusammentreffen und ob und welche Daten nach § 45d Abs. 1 und § 45e des Einkommenssteuergesetzes an das Bundeszentralamt für Steuern übermittelt worden sind. Diese Überprüfung findet zum 1. Januar, 1. April, 1. Juli und 1. Oktober statt.

Gemäß § 52 Abs. 4 SGB II wurde das Bundesministerium für Arbeit und Soziales ermächtigt, durch Rechtsverordnung das Nähere über das Verfahren des automatisierten Datenabgleichs zu regeln. Auf Grund dieser Ermächtigung wurde die Grundsicherungs-Datenabgleichsverordnung (GrSiDAV) erlassen. In dieser Verordnung ist das Verfahren bei den Auskunftsstellen und der Datenstelle der Träger der Rentenversicherung geregelt. Danach gleicht das Bundeszentralamt für Steuern die ihm übermittelten Daten mit den bei ihm gespeicherten Daten ab zur Feststellung von Kapitalerträgen, für die ein Freistellungsauftrag erteilt worden ist, und von Namen und Anschrift des Empfängers des Freistellungsauftrages (§ 2 Abs. 4 Nr. 1 GrSiDAV). Weiterhin gleicht die Datenstelle der Träger der Rentenversicherung die ihr übermittelten Daten mit den bei ihr gespeicherten Daten ab zur Feststellung von Zeiten einer geringfügigen Beschäftigung und einer versicherungspflichtigen Beschäftigung, zur Feststellung der Betriebsnummer, des Namens und der Anschrift des Arbeitgebers sowie zur Feststellung des Bezugs von Leistungen der Grundsicherung für Arbeitssuchende im Abgleichzeitraum (§ 2 Abs. 6 GrSiDAV).

Im vorliegenden Fall wurden dem Jobcenter im Rahmen des gesetzlich zugelassenen Datenabgleichs Einkommen aus geringfügiger Beschäftigung und Zinseinnahmen für den Petenten sowie Beschäftigungszeiten und Zinseinnahmen für eine der Bedarfsgemeinschaft angehörende Person gemeldet. Die Prüfung des Sachverhalts ergab, dass das Vorgehen des Jobcenters und der Umfang der Datenübermittlung den genannten Regelungen entsprachen, sodass für einen Datenschutzverstoß keine Anhaltspunkte bestanden.

Das Bundessozialgericht hat im Übrigen mit Urteil vom 24. April 2015 (Az. B 4 AS 39/14 R, juris) den automatisierten Datenabgleich des SGB II-Trägers mit dem Bundeszentralamt für Steuern für verfassungsgemäß erklärt.

11.2.4 Direktzahlung der Jobcenter an Dienstleister

Im Berichtszeitraum beschwerten sich mehrere Petenten darüber, dass Jobcenter Direktzahlungen an Dienstleister wie Brennstofflieferanten oder Autowerkstätten vornahmen. Durch die Direktüberweisung wurde dem Dienstleister der Sozialleistungsbezug bekannt. Der Bezug von Sozialleistungen ist jedoch ein Sozialdatum, dessen Offenbarung durch das Jobcenter nur zulässig ist, wenn eine gesetzliche Offenbarungsbefugnis vorliegt oder der Leistungsbezieher eingewilligt hat (Bundessozialgericht, Urteil vom 25. Januar 2012, Az. B 14 AS 65/11 R, juris). Als gesetzliche Übermittlungsbefugnis kommt § 69 Abs. 1 Nr. 1, 2. Alt. SGB X in Betracht. Dann muss die Datenübermittlung der Erfüllung einer gesetzlichen Aufgabe des Leistungsträgers dienen. Sie muss darüber hinaus als besonderer Ausfluss des Verhältnismäßigkeitsgrundsatzes dazu insoweit erforderlich, schlichtweg alternativlos sein, um die Aufgabe rechtmäßig, vollständig und in angemessener Zeit erfüllen zu können. Bei einer Übermittlung an Dritte, die nicht als Leistungsträger dem Sozialgeheimnis unterliegen, bedarf es dabei einer besonderen Rechtfertigung. Ohne weitere besondere Umstände ist nicht erkennbar, weshalb eine Zahlung nicht an den Leistungsberechtigten zur Weiterleitung an den Dienstleister erfolgen kann. Ausnahmen wären lediglich denkbar, wenn eine Zahlung an den Dienstleister erfolgen soll, da die entsprechende Verwendung durch die leistungsberechtigte Person nicht sichergestellt ist. Diese Möglichkeit ist für die Bedarfe für Unterkunft und Heizung nach § 22 Abs. 7 SGB II ausdrücklich geregelt und wegen des Grundsatzes der Förderung der Eigenverantwortung und des Grundrechts der Leistungsberechtigten auf informationelle Selbstbestimmung restriktiv auszulegen und anzuwenden. Die leistungsberechtigte Person ist über die Zahlung an Dritte schriftlich zu informieren (§ 22 Abs. 7 Satz 4 SGB II).

Besteht keine gesetzliche Offenbarungsbefugnis, ist eine Direktüberweisung an den Dienstleister nur dann datenschutzrechtlich unbedenklich, wenn eine Einwilligungserklärung des Leistungsberechtigten vorliegt. Die beteiligten Jobcenter haben erklärt, nunmehr auch alternative Zahlungsmöglichkeiten vorzusehen und die Leistungsberechtigten bereits im Antragsformular über die verschiedenen Möglichkeiten zu informieren.

11.2.5 Nutzung einer Vermieterbescheinigung durch Jobcenter

Mit der Nutzung einer Vermieterbescheinigung bzw. „Mietbescheinigung“, mit der auch der Vermieter Angaben zur Wohnung des Antragstellers machen bzw. bestätigen soll, hat sich der Landesbeauftragte bereits im X. Tätigkeitsbericht (Nr. 22.2) kritisch auseinandergesetzt. Trotzdem kam es auch im Berichtszeitraum wieder zu einer Beschwerde über die Nutzung einer Vermieterbescheinigung. Der Petent bemängelte insbesondere, dass sogar das Bestehen eines Verwandtschaftsverhältnisses zwischen Vermieter und Mieter und die Art des Verwandtschaftsverhältnisses anzugeben waren. Die Prüfung der Vermieterbescheinigung ergab außerdem, dass die Bankverbindung des Vermieters standardmäßig abgefragt wurde. Das Jobcenter erklärte, die Bankverbindung für den Fall von Mietrückständen zu benötigen. Die Angabe des Verwandtschaftsverhältnisses wollte das Jobcenter als freiwillig kennzeichnen, um leistungsberechtigte Personen mit Mietverträgen zu nahen Angehörigen nicht unter den Generalverdacht des Leistungsmissbrauchs zu stellen. Der Landesbeauftragte wies das Jobcenter in Bezug auf die Bankverbindung auf die unzulässige

Vorratsdatenhaltung und die grundsätzlichen Bedenken bei der Verwendung der Vermieterbescheinigung hin. So werden in einer Vielzahl von Fällen personenbezogene Daten zur Wohnungssituation erhoben, die zur Feststellung der angemessenen tatsächlichen Aufwendungen für Unterkunft und Heizung nicht erforderlich sind. Dies ist unverhältnismäßig und ein Verstoß gegen das Gebot der Datenvermeidung und Datensparsamkeit (§ 78b SGB X).

Im Übrigen sind Sozialdaten beim Betroffenen zu erheben (§ 67a Abs. 2 Satz 1 SGB X). Für die standardmäßige Nutzung einer Vermieterbescheinigung bei allen Antragstellern mit Mietverhältnissen besteht keine Veranlassung. Das Jobcenter teilte dem Landesbeauftragten mit, die Vermieterbescheinigung ab sofort nicht mehr zu verwenden und das Formular von der Homepage zu entfernen. Darüber hinaus werde das Jobcenter die für die Zahlung der Kosten der Unterkunft und Heizung erforderlichen Daten zukünftig zunächst bei den Betroffenen erheben.

11.2.6 Schweigepflichtentbindung für die Unfallversicherung

Ein Unfallversicherungsträger forderte von einem als Arzt tätigen Petenten vollständige Krankenblätter ab und legte eine Schweigepflichtentbindung des Patienten vor, die nach Auffassung des Arztes zu pauschal und damit unwirksam war. Der Arzt wies auch darauf hin, dass individuelle, namentlich auf den von der Schweigepflicht zu entbindenden Arzt ausgestellte und den konkreten Anlass und Umfang der Schweigepflichtentbindung benennende Schweigepflichtentbindungen erforderlich seien. Der Arzt bat um Einschätzung, ob die vorgelegte Schweigepflichtentbindung datenschutzrechtlichen Anforderungen genügt.

Der Landesbeauftragte für den Datenschutz wies den Petenten auf Folgendes hin: Nach § 203 Abs. 1 SGB VII sind Ärzte und Zahnärzte, die nicht an einer Heilbehandlung nach § 34 SGB VII beteiligt sind, verpflichtet, dem Unfallversicherungsträger auf Verlangen Auskunft über die Behandlung, den Zustand sowie Erkrankungen und frühere Erkrankungen des Versicherten erteilen, soweit dies für die Heilbehandlung und die Erbringung sonstiger Leistungen erforderlich ist. Das bedeutet, dass es bei Anfragen von Unfallversicherungsträgern wegen des Vorliegens einer Offenbarungsbefugnis einer Schweigepflichtentbindung des Versicherten nicht bedarf.

Grundsätzlich soll der Unfallversicherungsträger das Auskunftsersuchen auf solche Erkrankungen oder solche Bereiche von Erkrankungen beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können (§ 203 Abs. 1 Satz 2 SGB VII). In besonderen Fällen kann von einer Begrenzung des Auskunftsverlangens abgesehen werden, weil es sich um eine sogenannte Soll-Vorschrift handelt. Im vorliegenden Fall hat der Unfallversicherungsträger sodann gegenüber dem Arzt und dem Landesbeauftragten begründet, weshalb die Übersendung der vollständigen medizinischen Unterlagen erforderlich ist. Ein besonderer Fall lag also vor. Der Unfallversicherungsträger hat den Sachverhalt zum Anlass genommen, das Auskunftsersuchen nach Rücksprache mit dem behördlichen Datenschutzbeauftragten zu konkretisieren und seine mit der Bearbeitung von Versicherungsfällen betrauten Mitarbeiter und Mitarbeiterinnen auf die bestehende Rechtslage bei der Anforderung medizinischer Unterlagen hinzuweisen.

11.2.7 Akteneinsicht beim Jugendamt

Ein Vater beklagte sich beim Landesbeauftragten, da seine Akteneinsichtsanträge beim Jugendamt abgelehnt wurden. Das Jugendamt hatte gegenüber dem Gericht eine Stellungnahme im Verfahren um elterliche Sorge abgegeben.

Das Jugendamt verwies knapp und pauschal in seiner Stellungnahme gegenüber dem Landesbeauftragten darauf, dass es zum Petenten eigentlich keine Jugendamtsakte gebe. Relevanter Schriftverkehr sei ihm schon über das Gerichtsverfahren bekannt. Im Verlauf des Vorgangs wurden dem Jugendamt Informationen zugetragen, die keinesfalls kritik- oder kommentarlos dem Kindesvater überlassen werden könnten. Zum Teil stünden sie nicht im Zusammenhang mit dem Gegenstand des Verfahrens. Die Informationen seien zudem nach § 65 SGB VIII als sog. „anvertraute“ Daten vor der Weitergabe geschützt. Auch handele es sich vorwiegend um handschriftliche Notizen der Bearbeiterin, die als Entwürfe bzw. Vorarbeiten nach den Regeln der §§ 25 und 83 SGB X zur Geheimhaltung wegen schutzwürdiger Interessen Dritter ohnehin keiner Einsicht zugänglich wären.

Grundlagen der Akteneinsicht

Seitens des Landesbeauftragten wurde darauf hingewiesen, dass es verschiedene Grundlagen für den Zugang zu Akteninformationen gibt (§ 25 SGB X, § 83 SGB X, Akteneinsicht nach pflichtgemäßem Ermessen, IZG LSA). Die genannten Ausschlussgründe erscheinen oftmals aus Sicht der Jugendamtssachbearbeitung naheliegend, sind jedoch zumeist nicht einschlägig.

Zunächst darf nicht übersehen werden, dass nach dem *IZG LSA* für jedermann grundsätzlich ein Zugang zu amtlichen Informationen besteht. Daher ist stets auch zu prüfen, ob das Begehren auf Zugang zu Informationen als ein Antrag nach dem IZG LSA zu werten ist. Der Anspruch nach dem IZG LSA kann weiter gehen als nach dem Verfahrensrecht, wäre aber ggf. kostenpflichtig. § 5 IZG LSA, der eine Güterabwägung des Informationsinteresses des Antragstellers mit dem schutzwürdigen Interesse von Dritten zum Schutz personenbezogener Daten erfordert, dürfte jedoch im Sozialleistungsbereich häufig einem erfolgreichen Anspruch entgegenstehen. Der Schutz des Sozialgeheimnisses bleibt durch § 3 Abs. 1 Nr. 4 IZG LSA gewährleistet.

Das Recht auf Akteneinsicht nach *§ 25 SGB X* dient dem Zugang zu Behördeninformationen, soweit dies zur Geltendmachung bzw. Verteidigung der rechtlichen Interessen des Antragstellers erforderlich ist. Dieser gesetzliche Akteneinsichtsanspruch greift, wenn die Einsichtnahme bezweckt, eine tatsächliche Unsicherheit über ein Rechtsverhältnis zu klären, ein rechtlich relevantes Verhalten nach der Einsicht zu bewirken oder eine Grundlage für die Verfolgung von Ansprüchen zu erhalten. Rein berechtigte Interessen (wirtschaftlich, ideell) reichen nicht aus. Hintergrund dieser verwaltungsverfahrensrechtlichen Regelung ist die Gewährleistung des Rechtsstaatsprinzips, das den Beteiligten Anspruch auf rechtliches Gehör und ein faires Verfahren zusichert. Die Meinung der Behörde, dass es auf die Informationen sachlich nicht ankommt, spielt für den Zugang daher keine Rolle.

Der Anspruch auf Akteneinsicht steht nur den sogenannten Beteiligten eines Verwaltungsverfahrens zu, das auf den Abschluss durch Verwaltungsakt oder verwaltungsrechtlichen Vertrag gerichtet ist. Dies betrifft den Antragsteller, den Adressaten eines

beabsichtigten Verwaltungsaktes bzw. den Vertragspartner. Weiter kann die Behörde durch Verwaltungsakte weitere Personen als Beteiligte hinzuziehen. Andere in das Verfahren einbezogene Personen, wie z. B. Zeugen oder Sachverständige, haben keinen Beteiligtenstatus (§ 12 Abs. 3 SGB X, § 13 Abs. 3 VwVfG: Wer anzuhören ist, ohne dass die Voraussetzungen des Abs. 1 vorliegen, wird dadurch nicht Beteiligter).

Wenn die Beteiligten sich durch einen Bevollmächtigten vertreten lassen, können auch die Bevollmächtigten Akteneinsicht erhalten (§ 14 Abs. 1 VwVfG).

Es lag kein Sozialverwaltungsverfahren vor. In Verfahren nach § 162 FamFG stellt sich die Mitwirkung des Jugendamtes als eigene Aufgabe nach § 50 SGB VIII dar. Das Jugendamt handelt in Erfüllung eigener Aufgaben, die es nach seinen eigenen gesetzlichen Befugnissen zu erfüllen hat. Die Aufgaben sind in § 50 Abs. 2 SGB VIII beschrieben (Unterrichtung über erbrachte Leistungen, erzieherische und soziale Gesichtspunkte und weitere Möglichkeiten der Hilfe sowie ggf. über den Stand von Beratungsprozessen). Die Mitwirkung erfolgt grundsätzlich durch schriftliche Stellungnahme gegenüber dem Gericht. Die Datenerhebung für die Mitwirkung an Gerichtsverfahren erfolgt allerdings nicht auf der Grundlage des § 50 SGB VIII, der keine Befugnisnorm darstellt. Grundlage der Erhebung ist auch hier der § 62 SGB VIII (eine Verpflichtung zur Mitwirkung von Personen, die anzuhören wären, besteht aber nicht).

Auch wenn anlässlich der Mitwirkung des Jugendamtes in Gerichtsverfahren nach § 50 SGB VIII bei den Eltern bzw. Kindern Daten erhoben worden sind, werden die Betroffenen nicht Beteiligte eines Verwaltungsverfahrens. Ein Anspruch auf Akteneinsicht aufgrund des verwaltungsverfahrensrechtlichen Anspruchs aus § 25 SGB X kommt daher nicht in Betracht.

Eine weitere Rechtsgrundlage, die Zugang zu Akteninformationen gewähren kann, ist *§ 83 SGB X*. Danach ist dem Betroffenen Auskunft, also nicht notwendig Akteneinsicht, zu den zu seiner Person gespeicherten Sozialdaten auch in Bezug auf Herkunft und Empfänger zu geben. Dieser Anspruch basiert auf dem Grundrecht auf informationelle Selbstbestimmung, das dem Betroffenen das Recht gibt, zu wissen, welche Information eine öffentliche Stelle über ihn hat. Voraussetzung des Auskunftsanspruchs ist daher, dass es sich um Daten handelt, die sich auf den Antragsteller beziehen, also alle Angaben über persönliche und sachliche Verhältnisse des Betroffenen sowie seine Betriebs- und Geschäftsgeheimnisse (nach § 35 Abs. 4 SGB I gleichgestellt).

Bei der Prüfung eines derartigen Auskunftsanspruchs ist jedoch zu berücksichtigen, dass das Auskunftsrecht nicht schon dadurch ausgeschlossen wird, dass die Sozialdaten einen Doppelbezug aufweisen. Vom Auskunftsanspruch können daher durchaus auch Informationen erfasst sein, die Sozialdatenbezug zu anderen Personen beinhalten. Gerade bei häufig vorkommenden Dreiecksverhältnissen (Mutter – Vater – Kind), z. B. bei Sorgerechts- oder Umgangsverfahren, ist oft damit zu rechnen, dass Informationen in Bezug auf eine Person auch ein persönliches oder sachliches Verhältnis in Bezug auf eine andere Person darstellen. Soweit also z. B. der Kindesvater einen Antrag auf Akteneinsicht in einem Vorgang zur Vorbereitung einer Mitwirkung gegenüber dem Familiengericht stellt, ist im Hinblick auf einzelne Informationen zu Mutter oder Kind jeweils zu überprüfen, ob damit auch eine Aussage in Bezug auf ein sachliches Verhältnis des Vaters getroffen wird.

Auch nach der Auffassung des OVG Koblenz (Beschluss vom 16. Mai 2013, Az. 12 F 10369/13.OVG, juris) ist der Kindesvater als Antragsteller ebenso wie die Mutter kein außenstehender Dritter, sondern zumindest von der Mitwirkung des Jugendamtes mit betroffen.

Als weitere Grundlage für die Gewährung von Akteneinsicht in den Fällen, in denen eine Beteiligtenstellung im Verwaltungsverfahren nicht gegeben ist, kommt die Entscheidung über die *Akteneinsicht nach pflichtgemäßem Ermessen* in Betracht. Insoweit hat der Antragsteller einen Anspruch auf ermessensfehlerfreie Entscheidung über die Gewährung von Akteneinsicht. Dabei ist das Informationsinteresse des Antragstellers und das Schutzinteresse in Bezug auf sensible Daten Dritter sorgfältig abzuwägen. Demgemäß wäre nach den Vorgaben des § 25 Abs. 3 und § 83 Abs. 4 Nr. 3 SGB X auch beim Anspruch auf Einsicht nach Ermessen zu berücksichtigen, ob wegen überwiegender berechtigter Interessen Dritter Vorgänge geheim gehalten werden müssen. Allerdings sind die Vorschriften wegen ihres Charakters als Ausnahme gegenüber der Akteneinsicht restriktiv zu interpretieren.

Geheimhaltung

Die Frage der Geheimhaltung betrifft letztlich das Sozialdatengeheimnis. Eine Geheimhaltung ist daher grundsätzlich vorgegeben (§ 35 SGB I), kommt dann aber nicht in Betracht, wenn für die Behörde eine Übermittlungsbefugnis nach dem Sozialdatenschutzrecht gegeben ist. Dem Merkmal der Geheimhaltung kommt über das Sozialgeheimnis hinaus keine zusätzliche rechtliche Bedeutung zu. Maßgeblich sind daher die §§ 35 SGB I, 67d bis 77 SGB X sowie hier spezialgesetzlich §§ 64 und 65 SGB VIII. Demgemäß kann die Behörde nicht über die Regelungen des Sozialdatenschutzes hinaus Erwägungen anstellen, ob Vorgänge geheim zu halten sind.

Für die Übermittlung von Informationen für Verfahren nach § 162 FamFG ist demnach auf § 64 Abs. 2 SGB VIII in Verbindung mit § 69 Abs. 1 Nr. 1 SGB X abzustellen. Danach ist vorbehaltlich der Gefährdung des Leistungserfolges eine Übermittlung zur Erfüllung von Aufgaben des Jugendamtes zulässig. Soweit es daher für die Erfüllung der Aufgabe der Mitwirkung in gerichtlichen Verfahren nach § 50 SGB VIII erforderlich ist, kommt daher grundsätzlich die Übermittlung personenbezogener Sozialdaten an das Gericht durch das Jugendamt in Betracht.

Auch der besondere Vertrauensschutz in der persönlichen erzieherischen Hilfe nach § 65 SGB VIII hindert zumeist nicht eine Übermittlung von Informationen in Verfahren nach § 50 SGB VIII. Der häufige Einwand, dass die Weitergabe von Informationen z. B. zu Mutter oder Kindern an den antragstellenden Kindesvater nicht möglich sei, da es sich ja schließlich um sogenannte „anvertraute“ Daten handele, geht zumeist fehl. Von anvertrauten Daten kann erst dann ausgegangen werden, wenn die Daten einem Mitarbeiter des Jugendamtes im Vertrauen auf seine besondere Schutzpflicht nach § 65 SGB VIII in der Erwartung mitgeteilt worden sind, dass diese Informationen Dritten nicht zugänglich sind. Der Mitarbeiter muss also dem Betroffenen die besondere Schutzpflicht erklärt und klargestellt haben, in welcher Rolle er dem Betroffenen entgegentritt. Ob der Betroffene den Jugendamtsmitarbeiter ausdrücklich darauf hingewiesen haben muss, dass es sich um Informationen handelt, die höchstvertraulich sind und keinem Dritten zur Kenntnis gegeben werden dürfen, wird kontrovers diskutiert. Jedenfalls dürften die Informationen betroffen sein, die der Beschäftigte nicht erhalten hätte, wenn der Betroffene mit der Weitergabe hätte rechnen

müssen. Ein „Anvertrauen“ liegt daher nicht vor, wenn der Betroffene weiß oder ggf. wissen muss, dass seitens des Jugendamtes die mitgeteilten Informationen im Rahmen der Aufgabenstellung nach § 50 SGB VIII dem Gericht mitzuteilen sind (vgl. OVG Koblenz, a. a. O.).

Insgesamt ist daher zu würdigen, ob und inwieweit die einzelnen Informationen im Zusammenhang mit dem Dreiecksverhältnis Vater – Mutter – Kind und gerichtlichen Verfahren nach § 162 FamFG stehen oder ob eher individuelle höchst vertrauliche Beratungsinhalte in Bezug auf nur eine Person gegeben sind, die allen anderen Personen gegenüber nicht zugänglich sind. Zur Vermeidung von Problemen bei später durchzuführenden Akteneinsichten sollte versucht werden, bereits zu Beginn konkreter Vorgänge zu differenzieren zwischen der allgemeinen Aufgabenwahrnehmung des Jugendamtes in Bezug auf angebotene und erbrachte Leistungen, erzieherische und soziale Gesichtspunkte zur Entwicklung von Kindern und Jugendlichen sowie Beratungsprozesse mit Relevanz für gerichtliche Verfahren nach § 50 SGB VIII und den wenigen speziellen Vorgängen besonderen Vertrauensschutzes nach § 65 SGB VIII, die selbst Vorgesetzen und Rechnungsprüfungen grundsätzlich nicht zugänglich sind.

Entscheidungsentwürfe

Entgegen häufiger Einschätzung ergeben sich in der Regel keine Einschränkungen aus § 25 Abs. 1 Satz 2 SGB X, wonach Akteneinsichtsrechte keine Entwürfe zu Entscheidungen und Arbeiten zu deren unmittelbarer Vorbereitung erfassen. Der Einwand, dass handschriftliche Vermerke und Notizen zu Gesprächen hierunter fallen würden, trifft in der Regel nicht zu.

Sinn und Zweck der Regelung war, die Akteneinsicht in und die Diskussion über diverse Entwürfe zu Entscheidungen zu vermeiden, die so möglicherweise im Ergebnis nicht getroffen werden. Dabei geht es also um die Frage, wie Sachverhalte bewertet werden sollen. Die Feststellung des Sachverhaltes selbst sollte daher nicht der Einsicht entzogen werden. Nicht als Entscheidungsentwürfe sind daher Aktenvermerke, Berichte, Gutachten oder Stellungnahmen anderer Behörden zu sehen. Handschriftliche „persönliche“ Notizen (z. B. auf Klebezetteln) insbesondere über tatsächliche Sachverhalte können daher lediglich dann dem Vorgang und damit der Akteneinsicht entzogen werden, wenn die vorgangsrelevanten Tatsachen nach einem Gespräch z. B. in Vermerkform (abgetippt) inhaltlich umfassend formal der Akte zugefügt werden. Dies entspricht der gebotenen Dokumentation des Verwaltungsvorgehens.

11.2.8 Arbeitgebernachweis über die Nichtgenehmigung von Urlaub

Eine Petentin beschwerte sich beim Landesbeauftragten über die Datenerhebung einer städtischen Kindertagesstätte (Kita) im Rahmen der Schließzeiten. Mit einem Aushang informierte die Kita die Eltern nicht nur über die Schließzeiten der Kita, sondern auch, dass während dieser Schließzeiten Plätze in anderen Einrichtungen zur Verfügung gestellt würden, sofern die Nichtgewährung von Urlaub durch den Arbeitgeber oder die Ausbildungsstätte nachgewiesen wird. Da die Stadt Träger mehrerer Kitas und nicht auszuschließen war, dass das Prozedere in allen diesen Kitas erfolgte, bat der Landesbeauftragte die Stadt unter Hinweis auf den Erforderlichkeitsgrundsatz um Stellungnahme. Die Stadt legte dar, dass nur eine Kita den Bedarf durch einen Arbeitgebernachweis nachgewiesen haben wollte. Darüber hinaus räum-

te sie ein, dass im Rahmen der Bedarfserhebung für die Schließzeiten eine Elternanmeldung ausreichend und damit ein Arbeitgebernachweis über die Nichtgenehmigung von Urlaub im Sinne des § 62 Abs. 1 SGB VIII nicht erforderlich sei. Alle Einrichtungsleiterinnen wurden von der Stadt darauf nochmals entsprechend hingewiesen. Der Landesbeauftragte hat ergänzend empfohlen, die bereits erhobenen Arbeitgebernachweise mangels Erforderlichkeit gem. § 61 Abs. 1 SGB VIII i. V. m. § 84 Abs. 2 SGB X unverzüglich zu löschen.

11.2.9 Ambulant betreute Wohngruppen

Pflegebedürftige Menschen, die ihren Lebensalltag nicht mehr allein bewältigen können oder möchten, können in einer ambulant betreuten Wohngruppe in der Nähe ihres angestammten Wohnumfeldes gemeinschaftliche Pflege erhalten. Mit dem Pflegeneuausrichtungsgesetz hat der Gesetzgeber entschieden, diese Form der gemeinschaftlichen Pflege und Betreuung mit der Einführung eines Wohngruppenzuschlags in § 38a SGB XI, den die für die Versicherten zuständige Pflegekasse auf Antrag zahlt, zu unterstützen.

Nicht geregelt war dagegen, aufgrund welcher Informationen die Pflegekassen die leistungsrechtlichen Voraussetzungen zu prüfen haben. Die gesetzlichen Grundlagen für die Datenerhebung beim Versicherten waren im § 94 Abs. 1 Nr. 3 SGB XI zu sehen. Danach dürfen die Pflegekassen personenbezogene Daten für Zwecke der Pflegeversicherung erheben, verarbeiten und nutzen, soweit dies z. B. für die Prüfung der Leistungspflicht und die Gewährung von Leistungen an Versicherte erforderlich ist. Welche Daten im Einzelnen jedoch erforderlich sind, blieb umstritten. Die Pflegekassen forderten in unterschiedlichem Maße Unterlagen an, um die Leistungsvoraussetzungen zu prüfen. Manche Pflegekassen forderten die Vorlage von Mietverträgen, von Arbeitsverträgen der Präsenzkraft, die Angabe der Namen, Geburtsdaten, Pflegekasse und Pflegestufe sämtlicher Mitbewohner, teilweise mit Unterschriften. Diese Neugier der Pflegekassen führte nicht nur in Sachsen-Anhalt, sondern auch in anderen Bundesländern zu Beschwerden und Anfragen. Der Landesbeauftragte hatte zunächst bei der seiner Zuständigkeit unterliegenden Pflegekasse auf eine datenschutzkonforme Datenerhebung hingewirkt.

Als der Gesetzgeber 2014 beschloss, den Leistungsanspruch auf den Wohngruppenzuschlag vor dem Hintergrund der gesammelten Erfahrungen weiterzuentwickeln und § 38a SGB XI im Ersten Gesetz zur Stärkung der pflegerischen Versorgung und zur Änderung weiterer Vorschriften (Erstes Pflegestärkungsgesetz – PSG I, BGBl. I S. 2222) zu ändern, regelte er gleichzeitig abschließend, welche Daten die Pflegekassen zur Feststellung der Anspruchsvoraussetzungen erheben, verarbeiten und nutzen und welche Unterlagen sie anfordern dürfen (§ 38a Abs. 2 SGB XI). Somit besteht für die Pflegekassen nun eine eindeutige, abgegrenzte, gesetzlich geregelte Erhebungsbefugnis.

11.2.10 Ermittlungen der Grundsicherungsbehörde

Ein Petent beschwerte sich über „massive Datenschutzverletzungen, Nötigung und Mobbing“ durch eine für Grundsicherung im Alter und bei Erwerbsminderung zuständige Behörde. Sowohl ihm als auch seinem Vermieter werde in unzulässiger Weise gedroht, wenn sie Fragen nicht beantworten und geforderte Unterlagen nicht beige-

bracht werden. Die Zahlung der ihm bewilligten Leistung sei bereits eingestellt worden; er bitte mitzuteilen, wie sein Vermieter und er sich gegen das Mobbing schützen können.

Zunächst wies der Landesbeauftragte darauf hin, dass sich derjenige an ihn wenden kann, der der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Sozialdaten in seinen Rechten verletzt worden zu sein (§ 81 Abs. 1 Nr. 2 SGB X). Einige der Beschwerden des Petenten betrafen jedoch den Umgang der Grundsicherungsbehörde mit personenbezogenen Daten des Vermieters. Daraufhin wandte sich der Vermieter ebenfalls schriftlich an den Landesbeauftragten.

Die vorgelegten Schreiben der Grundsicherungsbehörde ließen tatsächlich zunächst den Schluss zu, dass die Grundsicherungsbehörde über das Ziel hinausgeschossen sein könnte, durch die Unterlagen in die Lage versetzt zu werden, die Anspruchsvoraussetzungen nach dem SGB XII zu prüfen.

So sollte der Petent z. B. beantworten,

- wie lange er den Vermieter bereits kenne,
- wieso er sein Grundstück an den Vermieter verkauft habe,
- wie hoch der Kaufpreis war und den Kaufvertrag vorlegen,
- ob er den Mietvertrag nur geschlossen habe, um höhere Sozialleistungsansprüche geltend zu machen,
- ob er Zeugen benennen könne, die die Echtheit des Mietvertrags bezeugen können,
- ob es andere Mieter im Haus gebe und diese namentlich benennen,
- ob er Rechnungskopien bzw. Kontoauszüge manipuliert habe.

Der Vermieter sah sich u. a. folgenden Fragen ausgesetzt:

- wie lange er bereits den Mieter kenne,
- ob er mit der Tochter des Mieters liiert sei,
- seit wann er Eigentümer des vermieteten Grundstücks sei,
- wie es zum Kauf des Grundstücks kam und wie hoch der Kaufpreis gewesen sei,
- ob er in der Vergangenheit jemals Mieteinnahmen steuerrechtlich im Rahmen der Einkommenssteuererklärung ausgewiesen habe,
- ob es andere Mieter für Wohnungen des Grundstücks gebe, was mit Dokumenten zu belegen sei,
- welche Erfahrungen er mit anderen Vermietungen gemacht habe.

Verfahren, den Mieter betreffend

In ihrer Stellungnahme teilte die Grundsicherungsbehörde dem Landesbeauftragten zunächst mit, im Rahmen eines vom Petenten angestrengten Rechtsschutzverfahrens auf Übernahme höherer Mietkosten seien Mängel und Unstimmigkeiten festgestellt worden. So seien seit über einem Jahr die von der Grundsicherungsbehörde an den Petenten gezahlten Leistungen für Unterkunft und Heizung wohl nicht an den Vermieter weitergeleitet worden. Da der Vermieter eine datenschutzrechtliche Erklärung des Petenten verlangt habe, die ihn zur Auskunft zum Mietverhältnis legitimieren sollte, habe sich der Anfangsverdacht eines Scheinmietvertrages ergeben. Deshalb seien die weitergehenden Recherchen gerechtfertigt gewesen.

Die durch die Grundsicherungsbehörde gegebene Erklärung konnte jedoch die Erforderlichkeit einer Vielzahl der gestellten Fragen nicht nachweisen. In einem Beratungstermin vor Ort verschaffte sich der Landesbeauftragte einen Überblick über die dem Fall zugrunde liegenden Tatsachen. Dabei stellte sich heraus, dass der mietende Petent durch teilweise manipulierte Unterlagen und unzutreffende Angaben in seinen Anträgen die umfangreichen Nachfragen ausgelöst hatte. So liefen Abbuchungen für Nebenkosten der gemieteten Wohnung über das Konto der Tochter des Mieters, die wiederum Zahlungen des Mieters auf ihr Sparkonto als Ausgleich erhielt. Dies hatte der Petent nicht dargestellt, sodass die Grundsicherungsbehörde sich veranlasst sah, umfassend den Sachverhalt zu ermitteln.

Hierzu erläuterte der Landesbeauftragte, dass grundsätzlich die Erhebung personenbezogener Daten verboten sei und einen Grundrechtseingriff darstellt. Deshalb sei bei jedem Vorgang zu prüfen, ob eine Norm den Eingriff erlaubt (Verbot mit Erlaubnisvorbehalt). Der von der Grundsicherungsbehörde als Grundlage des Handelns in Spiel gebrachte § 20 SGB X regelt zwar den Untersuchungsgrundsatz und die Amtsermittlungspflicht. Dem steht jedoch der Persönlichkeitsschutz des Betroffenen gegenüber. Dabei stehen das Aufklärungsinteresse der Behörde und der Persönlichkeitsschutz des Betroffenen nicht gleichrangig gegenüber; der Persönlichkeitsschutz des Betroffenen genießt Vorrang. § 20 SGB X ist keine Erhebungsbefugnis. Die Regelungen des Sozialdatenschutzes als begrenzte Erhebungs- und Verarbeitungsbefugnisse (§ 67a ff. SGB X) gehen den Verfahrensvorgaben des Untersuchungsgrundsatzes vor (§ 37 Satz 3 SGB I).

Die Erhebung, Verarbeitung und Nutzung von Sozialdaten ist nur unter den Voraussetzungen des Zweiten Kapitels des SGB X zulässig. Dabei ist die Erforderlichkeit der Daten zu begründen. Erforderlich sind Angaben, die für die Erfüllung der Aufgaben unerlässlich sind. Diese Daten sind vorrangig beim Betroffenen zu erheben. Bestehen bezüglich der Angaben des Antragstellers Zweifel, ist an die Möglichkeit der Versagung der Leistung mangels Nachweises der Anspruchsvoraussetzungen zu denken. Zu einer Ausweitung der Ermittlungen, z. B. zu Daten anderer Mieter der Immobilie, berechtigen die Zweifel nicht. Die Grundsicherungsbehörde wurde darauf hingewiesen, dass wegen der Zweifel am Vorliegen tatsächlicher Mietaufwendungen bzw. der Hinweise auf Manipulationen der Unterlagen die diesbezüglichen Fragen der Grundsicherungsbehörde datenschutzrechtlich zulässig seien. Die weiteren Fragen zur Erhellung des Umfelds würden jedoch Bedenken begegnen.

Verfahren, den Vermieter betreffend

Zu den Ermittlungen zum Vermieter stellte sich die Frage, ob der Leistungsträger dem Vermieter den Sozialleistungsbezug offenbaren durfte. Es hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis, § 35 Abs. 1 Satz 1 SGB I). Als Form der Verarbeitung gilt auch die Übermittlung. Als Sozialdatum gilt auch das Faktum des Bezugs von Sozialleistungen. Dessen Offenbarung durch Leistungsträger ist nur zulässig, wenn der Leistungsbezieher eingewilligt hat oder eine gesetzliche Offenbarungsbefugnis vorliegt (Bundessozialgericht, Urteil vom 25. Januar 2012, Az. B 14 AS 65/11 R, juris). Dann ist der Grundsatz der vorrangigen Datenerhebung beim Betroffenen zu beachten (§ 67a Abs. 2 Satz 1 SGB X). Die Erhebung von Daten bei anderen Personen und Stellen als dem Betroffenen hat sich auf wenige Ausnahmen zu beschränken (§ 67a Abs. 2 Satz 2 SGB X). Hintergrund der

Regelung ist das sich aus dem Recht auf informationelle Selbstbestimmung ergebene Prinzip, dass der Betroffene „Herr seiner Daten“ bleiben soll und entsprechend dem Grundsatz der Transparenz in der Regel keine Datenerhebung und Datenübermittlung hinter seinem Rücken erfolgen soll (Bundessozialgericht, a. a. O.).

Hier wies die Grundsicherungsbehörde darauf hin, dass wegen der bestehenden Mietrückstände geprüft werden sollte, ob die Leistungen für die Unterkunft nach § 35 Abs. 1 Satz 3 SGB XII an den Vermieter zu zahlen waren. Dafür sei es notwendig gewesen, die für die Entscheidung über die Zahlung an den Vermieter erforderlichen Daten beim Vermieter zu erheben. Dies erschien mit Blick auf § 67a Abs. 2 Satz 2 Nr. 2 b) aa) SGB X datenschutzrechtlich zulässig. Die Erhebungen weiterer Daten, z. B. zu den Hintergründen des Grundstückskaufs, zu weiteren Mietern oder die Beziehung des Vermieters zum Mieter bzw. seiner Tochter sowie die Berücksichtigung der Mieteinnahmen in der Steuererklärung, sind für die Prüfung der Leistungspflichten jedoch nicht erforderlich. Die datenschutzrechtlichen Bedenken wurden der Grundsicherungsbehörde in einem Beratungsgespräch ausführlich erläutert und letztlich von dieser geteilt.

11.2.11 Datenübermittlung eines Sozialamtes

Ein Ehepaar beschwerte sich über den Umgang mit seinen Daten durch das Sozialamt eines Landkreises. Die Eheleute waren mit Entscheidungen des Sozialamtes des Landkreises nicht einverstanden. Gegen Zahlungsaufforderungen des Sozialamtes setzten sie sich mit Schreiben zur Wehr, die beim Sozialamt den Eindruck erweckten, diese Äußerungen könnten disziplinarwürdig sein. Das Sozialamt übermittelte die Schreiben an deren Dienstherrn, der diese zum Anlass nahm, ein Disziplinarverfahren einzuleiten.

Der Landkreis teilte auf Bitte um Stellungnahme zunächst mit, man habe sich nach pflichtgemäßer Prüfung entschlossen, den Dienstherrn über die Äußerungen zu informieren. Als Übermittlungsbefugnis nannte der Landkreis zunächst „pflichtgemäße Prüfung“, dann § 68 SGB X i. V. m. Art. 33 Abs. 4 GG und führte ergänzend aus, der Schutz der Staats- und Rechtsordnung durch Beamte werde im SGB X überhaupt nicht berücksichtigt.

Der Landesbeauftragte wies den Landkreis darauf hin, dass nach § 67b Abs. 1 Satz 1 SGB X die Verarbeitung von Sozialdaten nur zulässig ist, soweit die nachfolgenden Vorschriften oder eine andere Rechtsvorschrift im SGB es erlauben oder anordnen oder soweit der Betroffene eingewilligt hat. Eine Einwilligung hatte unstrittig nicht vorgelegen.

Für die Anwendung des § 68 SGB X war entgegen der Auffassung des Sozialamtes kein Raum. Danach dürfen zur Erfüllung der Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr und der Justizvollzugsanstalten im Einzelfall auf Ersuchen Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift, derzeitiger oder zukünftiger Aufenthaltsort sowie Daten zum Arbeitgeber übermittelt werden. Somit schied nicht nur eine Übermittlung aus eigener Initiative aus, die übermittelten Daten gingen auch über das zulässige Maß weit hinaus. Als Übermittlungsgrundlage konnte § 68 SGB X somit nicht herangezogen werden. Art. 33 Abs. 4 GG formuliert lediglich einen Funktionsvorbehalt im Sinne

einer institutionellen Garantie eines Berufsbeamtentums, stellt jedoch keine Erweiterung spezialgesetzlicher Übermittlungsbefugnisse des Sozialgesetzbuches dar.

Auch die vom Landesbeauftragten zusätzlich vorgenommene Erwägung, ob die Übermittlung unter dem Aspekt der Wahrnehmung berechtigter Interessen in Anlehnung an die Vorgaben des § 34 StGB gerechtfertigt gewesen sein könnte, trug nicht: Eine für die Anwendung der Vorschrift nötige gegenwärtige, nicht anders abwendbare Gefahr war nicht erkennbar. Die Übermittlung diente lediglich der Prüfung einer denkbaren Verletzung beamtenrechtlicher Dienst- und Treuepflichten und dienstrechtlicher Konsequenzen. Eine das Sozialgeheimnis aufhebende Wahrnehmung berechtigter Interessen im Sinne eines rechtfertigenden Notstandes war damit nicht zu begründen.

In diesem Fall ist der Landesbeauftragte von einem besonders schweren Datenschutzverstoß ausgegangen und hat diesen nach § 24 DSG LSA förmlich beanstandet.

12 Personalwesen

12.1 Personalmanagementsystem PROMIS

Im IX. (Nr. 17.2) und X. Tätigkeitsbericht (Nr. 18.2) wurde die Entwicklung des Projekts PROMIS dargestellt. Im XI. Tätigkeitsbericht (Nr. 4.4) wurde im Zusammenhang mit dem zentralen IT-Dienstleister auf PROMIS Bezug genommen. Das System ist inzwischen im Geschäftsbereich des Ministeriums der Finanzen im Einsatz. Der Landesbeauftragte wurde zu einigen weiteren Detailfragen der Nutzung des Systems beteiligt. Die datenschutzrechtlichen Anforderungen werden durch Datenverschlüsselung und ein differenziertes Rollen- und Berechtigungskonzept berücksichtigt. PROMIS bildet eine der Datenquellen für ein Data-Warehouse, mit dem Daten aus unterschiedlichen Datenquellen in anonymisierter und aggregierter Form aufbereitet werden.

Zwischenzeitlich wurde dem Landesbeauftragten der Entwurf eines Verfahrensverzeichnisses für das System PROMIS vorgelegt. Es dürfte sich als Grundlage für die jeweiligen verantwortlichen Stellen eignen. Wichtig ist die Vertraulichkeit des Systems durch die Berechtigungssystematik. Der Zugriff erfolgt durch Benutzergruppen, d. h. grundsätzlich durch die Ressorts. Deren Kopfstellen richten die Benutzer und Profile in Anpassung an die Erforderlichkeit für die Aufgabenerfüllung ein. Die Bearbeitungsvorgänge werden in Module differenziert (Personal, Organisation, Stelle). Die Zugriffsberechtigungen für die Personalverwaltung sind nach Aufgabenbedarf individuell zu prüfen. Die Zugriffe werden protokolliert, sodass grundsätzlich eine spätere datenschutzrechtliche Kontrolle ermöglicht wird. Allerdings ist die Benutzerkennung arbeitsplatzbezogen. Im Ministerium der Finanzen ist daher eine Dienstanweisung ergangen, wonach beim Verlassen des Zimmers ein passwortgeschützter Bildschirmschoner zu verwenden ist. Beim Thema User-Help-Desk ist man den Vorgaben des Landesbeauftragten gefolgt und hat auf einen externen Zugriff auf personenbezogene Daten auf dem Bildschirm des Hilfesuchenden verzichtet. Nur bei mehrfachen Fehlanwendungen ist eine Freischaltung möglich. Weiter muss zur Gewährleistung der Funktion des Gesamtsystems eine kleine Gruppe von Verfahrensbetreibern des Systems Zugriff haben, die im Finanzamt Dessau-Roßlau angesiedelt

sind. Dazu wurde seitens des Landesbeauftragten erläutert, dass übergreifende Zugangsmöglichkeiten grundsätzlich vermieden werden sollten.

Zudem wurde die Verschlüsselung aller Daten als aus Sicht des Landesbeauftragten wesentlicher Aspekt umgesetzt. Sie erfolgt mit einer Funktion innerhalb der Datenbank, bei der Übertragung von und zur Datenbank und beim Backup. Weiter konnte der Landesbeauftragte die Einzeldatenfelder einsehen, die sich nach Abfrage bei den Ressorts als für die automatisierte Personalverwaltung erforderlich gezeigt haben. Die einzelnen Datenfelder stehen dabei jeweils im Zusammenhang mit den umzusetzenden Einzelmaßnahmen der Personalverwaltung, wie etwa Meldung zur Sozialversicherung, Eingruppierung, Umsetzung, etc. Hierzu wurde darauf hingewiesen, dass die den Datenfeldern beigefügten Kurzbeschreibungen plausibel klingen und zumindest keine offensichtlichen Bedenken begründen. Im Einzelfall muss in der Praxis geprüft werden, ob sich ggf. einzelne Datenfelder als entbehrlich erweisen.

12.2 Informationssystem Sachsen-Anhalt

Auf der Grundlage von Daten u. a. aus dem Personalmanagementsystem PROMIS und aus Haushaltsverfahren entwickelte das Ministerium der Finanzen ein Informationssystem Sachsen-Anhalt (ISA). Als Instrument einer zentralen Datenauswertung wurde hierzu ein Data-Warehouse (DWH) genutzt. Anhand der Vielzahl von personal- und haushaltsbezogenen Daten des Landes sollen mittels ISA den Ressorts Führungsinformationen (FIS), den Abgeordneten Abgeordneteninformationen (AIS) und dem Bürger Informationen im Bürgerinformationssystem (BIS) bereitgestellt werden (vgl. zu den informationsfreiheitsrechtlichen Aspekten dieses Systems Nr. 6.3 des III. Tätigkeitsberichts des Landesbeauftragten für die Informationsfreiheit, LT-Drs. 6/4048).

Das DWH selbst verwendet ausschließlich anonymisierte bzw. aggregierte Personaldaten von den Datenquellen. Angaben, die Beschäftigte bestimmbar machen könnten, wie z. B. Personalnummer, Sozialversicherungsnummer, Adresse etc., werden nicht verwendet. Zudem erfolgt über Berechtigungsdaten, Rollen und Nutzer eine differenzierte Zugriffregelung. Es kann nach Haushaltsstellen, Titeln oder Dienststellen differenziert werden. Einzelauswertungen können Aussagen treffen über die Statusgruppen der Beschäftigten oder die Geschlechts- oder Altersstruktur. Eine Verknüpfung der jeweiligen Berichte ist technisch nicht möglich. Vor diesem Hintergrund kann davon ausgegangen werden, dass ein datenschutzrelevanter Personenbezug nicht gegeben ist.

12.3 Zeiterfassung mittels Fingerabdruck

Eine Beschäftigte einer Gemeinde beschwerte sich beim Landesbeauftragten über das neu installierte Zeiterfassungssystem mittels Fingerabdruck und monierte, dass von allen Beschäftigten die Fingerabdrucknahme verlangt und erst nach erheblichem Widerstand durch die Petentin eine Zeiterfassung mittels Transponder ermöglicht wurde. Die Gemeinde wurde bezüglich dieser Datenerhebung und -verarbeitung umfänglich über die Rechtsgrundlagen und Voraussetzungen beraten. Insbesondere wurde darauf hingewiesen, dass es sich bei biometrischen Merkmalen um personenbezogene Daten mit besonderer Sensibilität handelt. Deshalb sollte eine Nutzung für Zwecke der Zutrittskontrolle aus Verhältnismäßigkeitsgründen auf besondere Aus-

nahmefälle (z. B. in Sicherheitsbereichen) beschränkt bleiben. Für bloße Zwecke der Zeiterfassung sind biometrische Verfahren in der Regel mangels Erforderlichkeit nicht einsetzbar, da wesentlich weniger in das Persönlichkeitsrecht der Arbeitnehmer eingreifende Verfahren zur Verfügung stehen dürften.

Die Gemeinde stellte daraufhin das Verfahren teilweise um. Da das neue Zeiterfassungssystem beide Varianten, die Nutzung eines Transponders und des biometrischen Fingerabdrucks, ermöglichte, werden den Beschäftigten nun beide Alternativen angeboten, und diese können individuell und frei darüber entscheiden. Darüber hinaus sicherte die Gemeinde zu, alle technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit ergriffen zu haben. Unter diesen Voraussetzungen und einer umfassenden Aufklärung der Beschäftigten und der Freiwilligkeit bei der Einwilligung hielt der Landesbeauftragte das von der Gemeinde dargestellte Verfahren aus datenschutzrechtlicher Sicht für noch vertretbar.

12.4 Personaldatenverarbeitung mittels WhatsApp

Im Berichtszeitraum hat der Landesbeauftragte erfahren, dass Polizisten mit privaten Handys Fotos von Dienstplänen per WhatsApp an Gruppenmitglieder versenden. Eine dienstliche Weisung oder einen Zwang zur Anmeldung bei WhatsApp habe es nach Mitteilung der Dienststellenleitung nicht gegeben. Der Landesbeauftragte erläuterte, dass derzeit eine datenschutzkonforme Nutzung von WhatsApp nicht möglich sei (siehe oben, Nr. 5.10). Die grundsätzlichen Bedenken zum Einsatz von WhatsApp bestehen seitens des Landesbeauftragten aber auch und gerade bei einer Nutzung zur Übermittlung dienstlicher Informationen der Polizei des Landes Sachsen-Anhalt. Aufgrund der datenschutzrechtlichen Probleme, die sich mit der Nutzung von WhatsApp ergeben, insbesondere auch der fehlenden Einflussmöglichkeit des Dienstherrn, wurden das Personal und insbesondere die Führungskräfte durch das Ministerium belehrt, die Übermittlung von Personaldaten und Dienstplänen mittels WhatsApp zu unterlassen.

12.5 Mitarbeiterüberwachung bei Verkehrsbetrieben

Der Betriebsrat eines Verkehrsunternehmens überreichte Unterlagen zu einem Transportkontrollsystem. Das Transportkontrollsystem gestattete, gestützt auf GPS, detaillierte Fahrzeugdaten zu sehen und aufzuzeichnen. Sobald ein Fahrzeug in Betrieb gesetzt wird, werden Standort und Bewegungseigenschaften aufgezeichnet. Ein Rückschluss auf den Fahrer ist mit Hilfe dieses Systems nicht möglich. Es sind lediglich die Linie und die Zugnummer erkennbar. Allerdings verfügt der Betrieb auch über ein Personalsystem, das die einzelnen Fahrer und ihre Fahrzeiten aufführt. Mit Hilfe dieses Systems ist erkennbar, wann welcher Fahrer welchen Zug gefahren hat. Demgemäß besteht grundsätzlich mit Hilfe der beiden Programme die Möglichkeit, Fahrverhalten einzelner Fahrer zu ermitteln. Der Betriebsrat wollte Zugang zu dem Transportkontrollsystem, also der Fahrzeugdisposition, haben. So könne man anhand der Verspätungen an den Wendepunkten feststellen, ob die vorgegebenen Pausenzeiten eingehalten werden. Hier wäre es Aufgabe des Betriebsrates, einen Verstoß gegen Sozialvorschriften zu erkennen und auf Abhilfe hinzuwirken. Der Betriebsrat habe auch Zugang zum Personalsystem, in dem die Arbeitszeiten (Anfang und Ende, Pause), der Einsatzplan, die Zugnummern sowie die Wohnanschrift und bei deren freiwilliger Angabe die Telefonnummern der Beschäftigten erkennbar sind.

Seitens des Landesbeauftragten wurde auf die datenschutzrechtlichen Rahmenbedingungen hingewiesen. Nach § 3 Abs. 1 DSG LSA ist der Betrieb eine öffentliche Stelle, da er zu 100% von der Stadt getragen wird und die öffentliche Aufgabe des Personennahverkehrs wahrnimmt (Nr. 3.1.1.4 VV DSG LSA). Infolge des Wettbewerbs mit anderen Transportunternehmen gelten gemäß § 3 Abs. 2 Nr. 1 DSG LSA überwiegend Vorschriften des BDSG. Weiterhin wurde darauf hingewiesen, dass der Einsatz der beiden genannten Systeme der Beteiligung und Beratung durch die behördliche Datenschutzbeauftragte bedurft hätte. So war z. B. die Frage zu klären, ob für das Transportkontrollsystem eine Vorabkontrolle hätte durchgeführt werden müssen. Weiterhin wurde darauf hingewiesen, dass nach § 3 Abs. 2 Nr. 1 DSG LSA i. V. m. § 9 BDSG nebst Anlage technische und organisatorische Maßnahmen der Datensicherheit angezeigt waren. Auch hierbei wurde auf die Notwendigkeit der Beteiligung der behördlichen Datenschutzbeauftragten hingewiesen. Vorsorglich wurde dem Betriebsrat erläutert, dass ihm zumindest die Informationen zur privaten Wohnanschrift und Telefonnummer der Beschäftigten wohl sicher nicht zukämen.

Schwerpunkt der Erörterungen war jedoch der Umgang mit Beschäftigtendaten. Im Hinblick auf die zugrunde liegenden gesetzlichen Rahmenbedingungen für den Einsatz von Systemen, die die Überwachung von Mitarbeitern ermöglichen (§ 32 bzw. § 28 BDSG), wurde die Notwendigkeit des Schutzes des Persönlichkeitsrechtes der Arbeitnehmer erläutert. Zunächst ist bei der Bewertung von Ortungssystemen zu berücksichtigen, dass es durchaus vielfältige legitime Anliegen eines Arbeitgebers zur Beobachtung des Fuhrparks mit GPS-Geräten geben kann (Optimierung und Koordinierung des Fahrzeugeinsatzes, effiziente Kontrolle der Einhaltung vertraglicher Verpflichtungen, Nutzungskontrolle, Schutz von Sachwerten in Bezug auf Verbleib bei Diebstahl etc.). Der konkrete Zweck wäre dann jeweils detailliert zu bestimmen. Neben der Lokalisation der vorhandenen Fahrzeuge und der Koordination von deren Einsatz kann es daher auch in Betracht kommen, in Bezug auf Beschäftigte das Anliegen zu verfolgen, die Arbeitszeiteinhaltung zu überwachen, Abfahrts- und Ankunftszeiten sowie Fahrzeiten zu betrachten oder Pausenzeiten zu dokumentieren.

Demgegenüber ist das Persönlichkeitsrecht der betroffenen Beschäftigten in seinem gesamten Umfang zu würdigen. Weit jenseits zulässiger Beobachtungen durch den Arbeitgeber wären sicher private Verhaltensweisen. Auch wäre ein permanenter Kontrolldruck im Sinne einer Vollüberwachung ebenso zu vermeiden wie die Erstellung von differenzierten Bewegungs- oder Verhaltensprofilen. Im Hinblick auf die Verhältnismäßigkeit und die gebotene Datensparsamkeit ist jeweils in Bezug auf den einzelnen Zweck zu würdigen, ob dieser ggf. durch weniger einschränkende Maßnahmen ebenso erreicht werden kann. Ist z. B. nur das Auffinden eines Objektes bei Verlust vorgesehen, reicht es aus, das System erst im Fall des Verlustes einzuschalten. Wäre der aktuelle Aufenthalt von Bedeutung, reicht eine Echtzeitüberwachung ohne Aufzeichnung. Sind für bestimmte Aufgaben Wegenachweise zu dokumentieren, kann dagegen eine kurze Speicherdauer in Betracht kommen. Im Hinblick auf den konkreten Zweck gilt es auch, zweckfremde Überwachungsmöglichkeiten durch Ausgestaltung des Verfahrens zu vermeiden. Eine Verwendung von Daten aus dem organisatorischen Transportkontrollsystem in Verbindung mit einem System zur Personaldisposition zu Zwecken der Verhaltens- und Leistungskontrolle wäre daher grundsätzlich sehr bedenklich. Demgemäß wurde positiv bewertet, dass einerseits das organisatorische Transportkontrollsystem und andererseits das System zur Personaldisposition getrennt agieren. Dies allein reicht jedoch nicht aus, wenn dieselben

Mitarbeiter des Betriebes ohne Weiteres gleichzeitig auf beide Systeme zugreifen und entsprechende individuelle Verhaltensprofile erstellen können. Auch wenn in der verantwortlichen Stelle grundsätzlich beide Systeme zur Verfügung stehen, wurde zur Sicherung des Schutzes der Persönlichkeitsrechte der Beschäftigten empfohlen, durch entsprechend ausgestaltete Rollen und Berechtigungskonzepte auch in der Anwendung eine entsprechende Trennung zu gewährleisten (Fahrdienstleiter – Fahrzeugstandorte, Personalbewirtschaftung – Dienstplanorganisation).

Anderes mag gelten, wenn konkrete Anhaltspunkte für Fehlverhalten im Einzelfall vorliegen. Dies kann sich z. B. daraus ergeben, dass anhand der zunächst anonymen Fahrzeugüberwachung ersichtlich wird, dass an bestimmten Stellen oder in bestimmten Zeiten Geschwindigkeitsüberschreitungen o. ä. Verfehlungen auftreten. Überwachungen in zunächst anonymisierter oder pseudonymisierter Form gewährleisten die Verhältnismäßigkeit. Dies gibt Gelegenheit, gegenüber der Belegschaft darauf hinzuweisen, dass bestimmte fehlerhafte Verhaltensweisen auffällig geworden sind, die es zu unterlassen gilt. Verbunden werden könnte dies mit dem Hinweis darauf, dass bei wiederholtem Auftreten entsprechenden Fehlverhaltens eine personenbezogene Ermittlung unter Rückgriff auf das Personaldispositionssystem erfolgen müsse. Weiterhin dürfte eine beschäftigtenbezogene Überprüfung auch in Betracht kommen, wenn hinreichende Anhaltspunkte einen konkretisierten Verdacht auf mögliche Straftaten oder vergleichbare Vergehen hervorrufen. Hierzu hatte der Entwurf einer Betriebsvereinbarung bisher vorgesehen, dass in Ausnahmefällen eine Bewertung von Leistung und Verhalten von Beschäftigten vorgesehen werden kann. Zu diesem Ansatz wurde empfohlen, den Inhalt des Begriffs der Ausnahmefälle durch die Aufführung von konkreten Vorgaben oder zumindest von einschränkenden Beispielsfällen klarzustellen. Weiter ist zudem auf die Ausgestaltung eines angemessenen Verfahrens zu achten, z. B. durch Zugriffsbeschränkung. Auch insoweit wurde auf die notwendige Beteiligung der Datenschutzbeauftragten und des Betriebsrates hingewiesen. Es erscheint sinnvoll, konkretisierte Überwachungsmaßnahmen jeweils vorher mit dem Betriebsrat abzustimmen. Ergänzend sollte die Möglichkeit des Betriebsrates bestehen, in Protokollierungen zu Zugriffen Einsicht zu nehmen, um insoweit personenidentifizierende Überwachungsmaßnahmen über das legitime Maß hinaus feststellen zu können. Somit wird auch durch die Verfahrensausgestaltung ermöglicht, einer unverhältnismäßigen Beschäftigtenüberwachung entgegenzuwirken.

Von der angedachten Aufschaltung des Betriebsrates auf das System riet der Landesbeauftragte letztlich ab. Betriebsräte haben zwar wie Personalvertretungen gegenüber dem Unternehmen bzw. der Dienststelle das Recht, die für die Erfüllung ihrer Aufgaben notwendigen Informationen rechtzeitig und umfassend vorgelegt zu bekommen. Dies gibt jedoch keine Handhabe für allgemeine umfassende Vorabinformationen sowie Zugriffe auf Informationssysteme, deren Inhalt weit über das konkrete Aufgabengebiet hinausgeht.

Der Schwerpunkt des Interesses des Betriebsrates lag an dem möglichst konkreten Nachweis reduzierter Pausenzeiten an den Wendepunkten der Bus- und Straßenbahnlinien. Insoweit wäre jedoch zunächst zu prüfen, ob durch Ausdrucke der jeweiligen Ankunfts- und Abfahrtszeiten an den Wendepunkten ausreichende Möglichkeiten zur Überwachung der Einhaltung von Sozialvorschriften gegeben sind. Neben Ausdrucken kommen ggf. auch auszugsweise Einblicke in das Transportkontrollsystem in Betracht. Ein dauerhafter umfassender Überblick über die gesamten System-

dokumentationen, noch dazu verbunden mit der Möglichkeit der Kombination mit personenbeziehbaren Datenbanken, erschien jedoch zu weitreichend.

12.6 Mindestlohngesetz

Im Berichtszeitraum erhielt der Landesbeauftragte eine Anfrage der IHK Magdeburg zum Gesetz zur Regelung eines allgemeinen Mindestlohns – Mindestlohngesetz (MiLoG). Dieses Gesetz ist am 16. August 2014 in Kraft getreten. Es enthält in § 13 einen Verweis auf § 14 des Arbeitnehmerentsendegesetzes, wonach ein Unternehmer (Auftraggeber) letztendlich haftet, wenn einer seiner Subunternehmer (Auftragnehmer) seinen Beschäftigten nicht (mindestens) den Mindestlohn zahlt. Außerdem kann ein hohes Bußgeld verhängt werden, wenn ein Auftraggeber weiß oder fahrlässig nicht weiß, dass sein Auftragnehmer keinen Mindestlohn zahlt. Die IHK wollte wissen, ob ein Auftraggeber von seinen Auftragnehmern die Herausgabe der Verdienstbescheinigungen seiner Beschäftigten verlangen kann, um zu prüfen, ob auch tatsächlich Mindestlohn gezahlt wird.

Verdienstbescheinigungen enthalten eine Fülle von personenbezogenen Daten (i. d. R. Name, Vorname, Adresse, Arbeitgeber, Höhe des Bruttoverdienstes, Steuerklasse, Abzüge, ggf. Kirchensteuer). Die Erhebung dieser personenbezogenen Daten von Beschäftigten eines Auftragnehmers durch den Auftraggeber ist nur dann zulässig, soweit sie gemäß § 28 Abs. 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen des Auftraggebers erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Übermittlung überwiegt.

Zwar hat der Auftraggeber grundsätzlich ein berechtigtes Interesse, zu erfahren, ob der von ihm beauftragte Auftragnehmer die Vorgaben des MiLoG einhält. Schließlich hängen von der Beantwortung dieser Frage u. U. erhebliche Haftungsrisiken ab. Die Konferenz der Datenschutzbeauftragten sieht in ihrer Entschließung vom 18. Und 19. März 2015 die Einsichtnahme in Verdienstbescheinigungen oder gar Lohnlisten allerdings als nicht erforderlich an (**Anlage 25**). Der Auftraggeber verfügt über andere Möglichkeiten, um sicherzustellen, dass sein Auftragnehmer den Mindestlohn zahlt. In Betracht kämen z. B.:

- sorgfältige Auswahl von seriösen Auftragnehmern (Haftungsrisiko dürfte bei „Billiganbietern“ steigen),
- schriftliche Zusicherung des Auftragnehmers, den Mindestlohn zu zahlen,
- Gewährung von Sicherheiten für den Fall der Haftungsinanspruchnahme z. B. in Form einer Bankbürgschaft,
- vertraglich vereinbarte Regressregelungen für den Fall der Haftungsinanspruchnahme bzw. ein entsprechendes Vertragsstrafeversprechen.

Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar, bei denen der Auftraggeber keinen Personenbezug erkennen kann.

13 Finanzen, Kataster, Kommunales und Statistik

13.1 Entwicklung der Kontendatenabrufe

In vergangenen Tätigkeitsberichten, so im VII., VIII. und auch im IX. Tätigkeitsbericht, hat der Landesbeauftragte zur Problematik der rechtlichen Entwicklung der Kontendatenabrufe beim Bundeszentralamt für Steuern berichtet.

Den Beitrag Nr. 9.2 „Kontenabrufverfahren“ im IX. Tätigkeitsbericht – somit im Jahr 2009 – schloss der Landesbeauftragte mit der Feststellung, dass sich Kontendatenabrufe in Sachsen-Anhalt auf Einzelfälle beschränken. Diese Aussage kann für die aktuelle Entwicklung nicht mehr aufrechterhalten werden.

Gesetzesänderungen haben dazu geführt, dass seit 2013 nunmehr zusätzlich zu den Finanzämtern, Kommunen, Sozialämtern und Jobcentern auch die Unterhaltsvorschussstellen und die Gerichtsvollzieher Kontendaten beim Bundeszentralamt für Steuern abrufen dürfen. Von dieser gesetzlichen Möglichkeit wird umfangreich Gebrauch gemacht.

Die Zahlen über die erfolgten Kontendatenabrufe, die dem Landesbeauftragten monatlich zur Verfügung gestellt werden, zeigten eine extreme Zunahme von Kontendatenabrufen. Beliefen sich die erfolgten Abrufe nach § 93 Abs. 8 Abgabenordnung im Jahr 2012 noch auf monatlich unter zehn, waren es im Sommer 2013 monatlich bereits zwischen 200 und 300. Im Jahr 2014 waren es dann bereits im Schnitt 500 Kontendatenabfragen im Monat.

Ein Kontendatenabruf ist jedoch nach Gesetz an bestimmte Voraussetzungen gebunden. Der Landesbeauftragte hat in der Vergangenheit bereits bei den Finanzämtern geprüft, ob diese Behörden sich bei Kontendatenabfragen an die förmlichen Vorgaben halten und diese auch in ihren Akten nachweisen.

Der Landesbeauftragte beabsichtigt, solche Kontrollen im nächsten Berichtszeitraum auch auf die Gerichtsvollzieher auszudehnen.

13.2 Verarbeitung von Steuerdaten

In der Steuer- und Finanzverwaltung gibt es im Zusammenhang mit den Entwicklungen im E-Government seit vielen Jahren Bestrebungen, dass alle Arbeitsschritte im Zusammenhang mit der Steuererklärung automatisiert erfolgen können bzw. inzwischen sogar immer mehr Arbeitsschritte automatisiert erfolgen müssen.

Der Landesbeauftragte berichtete dazu auch in seinen Tätigkeitsberichten (so z. B. im VIII. Tätigkeitsbericht unter Nr. 8.5 und in seinem IX. Tätigkeitsbericht unter Nr. 9.6) über die zur damaligen Zeit aktuellen Entwicklungen.

Mit dem Projekt KONSENS (Koordinierte neue Softwareentwicklung der Steuerverwaltung) wurde ein auf Dauer angelegtes Vorhaben realisiert, durch welches Softwareprodukte für die Steuerverwaltung entwickelt wurden, die auch von allen Bundesländern genutzt werden. Eine der größten Entwicklungen in diesem Bereich ist das Verfahren ELSTER (Elektronische Steuererklärung), welches für die elektronische Übermittlung von Steuererklärungen und Steueranmeldungen genutzt wird.

Auch die Abschaffung der papiernen Lohnsteuerkarte durch das Projekt ElsterLohn II ist hierauf zurückzuführen.

Der Vorteil, der sich aus der Entwicklung solcher von allen Bundesländern genutzten einheitlichen Programme ergibt, liegt auf der Hand. Es müssen nunmehr bei Änderungen im Steuererhebungsrecht nicht mehr für alle genutzten IT-Verfahren eigene Programme zur Berechnung geschrieben werden.

Aber auch für die Finanzverwaltung werden auf diese Weise Synergieeffekte erzielt. Wie der Landesbeauftragte in seinem XI. Tätigkeitsbericht (Nr. 4.4) berichtete, hat sich das Land Sachsen-Anhalt entschlossen, neben Schleswig-Holstein, Hamburg, Mecklenburg-Vorpommern, Bremen und Niedersachsen Trägerland und Miteigentümer der rechtsfähigen Anstalt des Öffentlichen Rechts Dataport als zentraler IT-Dienstleister zu werden (siehe dazu Nr. 4.6).

Dataport betreibt für die Steuerverwaltung das gemeinsame Rechenzentrum Steuern in Rostock. Die einzelne Steuererklärung wird durch die Finanzbeamten des Landes in den Finanzämtern bearbeitet. Die eigentliche Berechnung, der Ausdruck und das Versenden der Steuererklärung erfolgt jedoch im Steuerrechenzentrum.

Damit auch dort die Einhaltung der datenschutzrechtlichen Vorschriften sichergestellt wird, wurden mit § 15 entsprechende Regelungen im Staatsvertrag aufgenommen, die eine Kontrolle auch durch den Landesbeauftragten ermöglichen. Des Weiteren finden regelmäßige Treffen der Datenschutzbeauftragten der Dataport-Trägerländer statt, um eine Abstimmung in wesentlichen Fragen zu gewährleisten und sich gegenseitig über neue Vorhaben oder Änderungen zu informieren (vgl. auch Nr. 4.6).

13.3 Fortführung des Liegenschaftskatasters

Das Liegenschaftskataster weist, so § 11 VermGeoG LSA, alle Liegenschaften in der Liegenschaftskarte darstellend und im Liegenschaftsbuch beschreibend nach, wobei auch ein Gebäude eine Liegenschaft im Sinne des Gesetzes sein soll. Um die Übereinstimmung des Liegenschaftskatasters (Theorie) mit der Wirklichkeit (Praxis) zu gewährleisten, hat der Gesetzgeber in § 14 Abs. 1 VermGeoG LSA die Eigentümer der Liegenschaften, die Erbbauberechtigten und die Inhaber weiterer grundstücksgleicher Rechte in die Pflicht genommen. Dieser Personenkreis hat der Vermessungs- und Geoinformationsbehörde die für die Führung des Liegenschaftskatasters notwendigen Angaben zu machen. Er hat nämlich die Behörde unverzüglich zu unterrichten, wenn z. B. ein Gebäude neu errichtet oder ein bestehendes Gebäude in seinen Ausmaßen verändert wurde. Ist die Vermessung des Gebäudes erforderlich, so hat sein Eigentümer nach § 14 Abs. 2 VermGeoG LSA diese Vermessung und die Übernahme der Ergebnisse in das Liegenschaftskataster zu veranlassen. Ein Teil der Eigentümer kennt diese Rechtspflichten nicht, ein anderer wird sie kennen, aber unter der unverzüglichen Unterrichtung der Behörde etwas anderes verstehen als der Gesetzgeber und das LVermGeo.

Um gleichwohl die Aktualität des Liegenschaftskatasters und seine Übereinstimmung mit der Wirklichkeit hinreichend sicherzustellen, hält das LVermGeo ergänzend zur antragsbezogenen Fortführung des Liegenschaftskatasters ständig Aktualitätsüberwachungen durch turnusmäßige Auswertungen von Luftbildern und Feldvergleiche für erforderlich. Hat der Gebäudeeigentümer keinen Antrag auf Fortführung des Lie-

genschaftskatasters beim LVermGeo gestellt, wird er ggf. von der Behörde durch Übersendung von allerlei Unterlagen auf seine Vermessungspflicht hingewiesen. Bei diesem datenschutzrechtlich an sich korrekten Verfahren sind dennoch Fehler möglich und mehrfach auch passiert, worüber sich die Betroffenen beim Landesbeauftragten beschwerten.

In einem Fall hatte ein Gebäudeeigentümer, der seinem Wohnhaus einen Wintergarten anfügen ließ, nicht nur vom LVermGeo die schriftliche Erinnerung erhalten, den Anbau vermessen zu lassen, sondern fast zeitgleich auch ein Angebot eines Vermessungsbetriebes, eben diese Vermessung auszuführen. Wohlgemerkt: zu einem Zeitpunkt, zu dem außer dem Bürger nur das LVermGeo von der erforderlichen Vermessung wusste. Mit dem Hinweis, dass das ja wohl nicht mit rechten Dingen zugehen könne, und der Frage, auf welche Rechtsgrundlage eine möglicherweise stattgefundene Übermittlung seiner personenbezogenen Daten vom LVermGeo an den Vermessungsbetrieb beruhte, wandte sich der Bürger an den Landesbeauftragten. Das LVermGeo, durch den Landesbeauftragten auf die merkwürdigen Umstände aufmerksam gemacht, führte eine interne Revision durch, konnte jedoch nach eigenem Bekunden keinen Hinweis darauf finden, dass personenbezogene Daten des Petenten an Dritte übermittelt wurden. Diese Übermittlung wäre nach Ansicht des Landesbeauftragten jedenfalls rechtswidrig gewesen, da weder eine Rechtsgrundlage noch eine Einwilligung des Betroffenen vorlagen. Das LVermGeo teilte dem Landesbeauftragten mit, dass die Mitarbeiter hinsichtlich des Verbotes der Weitergabe von internen Informationen besonders sensibilisiert worden seien. Es sei, und das ist der datenschutzrechtlich zu begrüßende Aspekt des Sachverhaltes, zusätzlich zur jährlichen Antikorruptionsbelehrung eine entsprechende aktenkundige Belehrung erfolgt.

Um es den Betroffenen so einfach wie möglich zu machen, dem LVermGeo die notwendigen Informationen und Angaben zuzuleiten, die dieses feststellen lassen können, ob eine Vermessungspflicht für ein Gebäude besteht, enthalten die o. g. Unterlagen des LVermGeo auch einen grafischen Nachweis der betreffenden Liegenschaft. Auf diesem Auszug aus der Liegenschaftskarte sind die möglicherweise vermessungspflichtigen Gebäude besonders markiert und ggf. nummeriert. In der Regel grenzen an ein Flurstück Nachbarflurstücke an. Auf diesen könnten sich vermessungspflichtige, aber noch nicht vermessene Gebäude des Nachbarn befinden. Auch diese Gebäude waren bei Bürgern, die sich an den Landesbeauftragten wandten, auf der Liegenschaftskarte, soweit der Nachbarbereich sichtbar war, farblich markiert. Damit war es Eigentümer A möglich, zu erkennen, dass sein Nachbar, Eigentümer B, ebenfalls pflichtwidrig nicht vermessene Gebäude auf seinem Grundstück hat.

Es sei dahingestellt, ob diese Information schutzwürdig ist oder nicht, jedenfalls wird sie bei natürlichen Personen ein personenbezogenes Datum darstellen. Der Umgang mit solchen personenbezogenen Daten regelt sich nach den einschlägigen Fachgesetzen, z. B. dem VermGeoG LSA oder ersatzweise nach dem DSG LSA. Das LVermGeo hatte keine Befugnis, personenbezogene Daten des Eigentümers A an den Eigentümer B und umgekehrt zu übermitteln, da weder Rechtsgrundlage noch Einwilligung erkennbar waren. Darum forderte der Landesbeauftragte das LVermGeo auf, gemeinsam mit seinem Beauftragten für den Datenschutz nach einer geänderten Verfahrensweise zu suchen, die die unzulässige Datenübermittlung fortan unterbindet. Zukünftig werden die Nachbargrundstücke auf den versandten Auszügen aus der Liegenschaftskarte ausgeblendet.

13.4 Kommunalverwaltung

13.4.1 Das neue Kommunalverfassungsgesetz

Im Tätigkeitsberichtszeitraum hat sich der Landesbeauftragte mit der Änderung des Kommunalverfassungsrechts befasst (zur informationszugangsrechtlichen Bewertung des Gesetzes vgl. Nr. 5.4.1 des III. Tätigkeitsberichts zur Informationsfreiheit). Dazu wurde dem Landesbeauftragten durch das Ministerium des Innern und Sport im Mai 2013 ein erster Entwurf vorgelegt. Ziel des neuen Kommunalverfassungsrechts ist, die bestehenden verschiedenen Kommunalgesetze wie die Gemeindeordnung, die Landkreisordnung und das Verbandsgemeindegesetz zu einem Kommunalverfassungsgesetz zusammenzufassen. Des Weiteren sollten Entwicklungen in der Praxis, die Rechtsprechung und Erfahrungen mit dem geltenden Recht berücksichtigt werden.

Aus datenschutzrechtlicher Sicht ist die ausdrückliche Zulassung der Medienöffentlichkeit zu öffentlichen Sitzungen der Vertretung und seiner Ausschüsse hervorzuheben. Bisher waren Bild- und Tonaufnahmen und Bild- und Tonübertragungen durch Presse, Rundfunk und ähnliche Medien nur möglich, wenn alle Beteiligten ihr zugestimmt haben. Nunmehr besteht für die Vertretung die Möglichkeit, in der Geschäftsordnung die näheren Bedingungen zur Zulassung von Bild- und Tonaufnahmen und von Bild- und Tonübertragungen durch Presse, Rundfunk und ähnliche Medien zu regeln.

Diese in § 52 Abs. 5 KVG LSA erfolgte grundsätzliche Öffnung von Bild- und Tonaufnahmen sowie Bild- und Tonübertragungen in öffentlichen Sitzungen der Vertretung ist ausdrücklich zu befürworten, da sie klarstellt, dass mit der Öffentlichkeit der Sitzung nicht nur die Saal-, sondern auch die Medienöffentlichkeit gemeint ist. Dieser Punkt wurde in Rechtsprechung und Lehre bisher kontrovers diskutiert (vgl. nur OVG Saarland, Beschluss vom 30. August 2010, Az. 3 B 203/10). Die von den kommunalen Spitzenverbänden an der Zulassung der Medienöffentlichkeit geäußerte grundsätzliche Kritik ist nicht mehr zeitgemäß. Die Öffentlichkeit der Sitzungen gehört zu den wesentlichen Grundsätzen der Kommunalverwaltung. Durch sie soll den Bürgerinnen und Bürgern die Möglichkeit gegeben werden, die Arbeit der gewählten Vertreter zu verfolgen und die Vorgänge in der Kommune allgemein zu kontrollieren (VG Magdeburg, Beschluss vom 9. Juli 2012, Az. 9 B 137/12). Die Übertragung der öffentlichen Sitzungen – auch ins Internet – ist daher ein ideales Mittel, um die gewollte Transparenz und bürgerschaftliche Kontrolle zu gewährleisten. Vor diesem Hintergrund hatte der Landesbeauftragte in der Anhörung zu dem Regierungsentwurf vorgeschlagen, die in § 52 Abs. 5 E-KVG LSA vorgesehene Medienöffentlichkeit in öffentlichen Sitzungen der Vertretung auch in öffentlichen Sitzungen der Ausschüsse grundsätzlich zuzulassen. Der Landesbeauftragte begrüßt es daher ausdrücklich, dass die Landesregierung seinem Vorschlag gefolgt ist (vgl. LT-Drs. 6/2247, S. 151, 152).

Unter datenschutzrechtlichen Gesichtspunkten bestehen gegen eine Bild- und Tonübertragung einer öffentlichen Sitzung auch grundsätzlich keine Bedenken, wenn das Kunsturhebergesetz beachtet wird. Klarstellende Regelungen hierzu können in der Geschäftsordnung getroffen werden.

Des Weiteren wurde in § 99 Abs. 6 KVG LSA klargestellt, dass das Einwerben von Spenden und Sponsoring durch den Hauptverwaltungsbeamten grundsätzlich zulässig ist. Über die Annahme oder die Vermittlung von Spenden, Schenkungen oder ähnlichen Zuwendungen ab einer in der Hauptsatzung festzulegenden Wertgrenze entscheidet dann die Vertretung in öffentlicher Sitzung. So wird unterstrichen, dass durch ein öffentliches Verfahren dem Verdacht der Vorteilsannahme bzw. der Bestechlichkeit von Mitarbeitern der Kommune entgegengewirkt werden soll. Aus diesem Grund ist aus datenschutzrechtlicher Sicht gegen eine Veröffentlichung von personenbezogenen Daten nichts einzuwenden.

Das Gesetz zur Reform des Kommunalverfassungsrechts des Landes Sachsen-Anhalt und zur Fortentwicklung sonstiger kommunalrechtlicher Vorschriften (Kommunalrechtsreformgesetz) ist zum 1. Juli 2014 in Kraft getreten.

13.4.2 Datenausspähung durch Sichtung des E-Mail-Verkehrs

In einer Verbandsgemeinde des Landes herrschen immer wieder Meinungsverschiedenheiten zwischen dem Verbandsgemeindebürgermeister und dem Verbandsgemeinderat.

Im Sommer 2012 eskalierte die Auseinandersetzung zwischen den Betroffenen so sehr, dass einzelne Ratsmitglieder die Abwesenheit des Verbandsgemeindebürgermeisters nutzten, um mehrere Beschlüsse der Verbandsgemeindevertretung herbeizuführen, nach welchen u. a. der gesamte E-Mail-Verkehr der Verbandsgemeinde durch eine IT-Firma auf einer Festplatte gesichert wurde.

Laut Antrag der Verbandsgemeindevertretung sollte diese Sicherung auch genutzt werden, um speziell den E-Mail-Verkehr des Verbandsgemeindebürgermeisters und einiger anderer Beschäftigter zu sichten und Disziplinarmaßnahmen gegen diese anzustrengen.

Als der Landesbeauftragte von diesen Vorgängen unterrichtet wurde, nahm er Kontakt mit der Kommunalaufsicht auf, um zu erfahren, wie die kommunalrechtliche Bewertung dieser Beschlüsse ausfiel. Von dort war zu erfahren, dass den infrage kommenden Beschlüssen bereits widersprochen wurde. Jedoch hatte die Datensicherung durch die IT-Firma bereits stattgefunden.

Der Landesbeauftragte bat somit die Firma um Stellungnahme, welche Maßnahmen konkret durchgeführt wurden und wer zurzeit diese „Datensicherung“ in den Händen hat. Dabei stellte sich heraus, dass die Daten auf eine externe Festplatte gespeichert wurden und diese Festplatte der behördlichen Datenschutzbeauftragten zur Verwahrung gegeben wurde. Die Datenschutzbeauftragte versicherte dem Landesbeauftragten auf Nachfrage, dass sich die Festplatte unter Verschluss befindet und nur sie allein den Zugang zur Festplatte hat. Dagegen erklärte der Verbandsgemeinderat gegenüber dem Landesbeauftragten, dass ein „Anlesen“ der E-Mails erfolgt sei. Allerdings sah sich der Verbandsgemeinderat als Dienstherr des Verbandsgemeindebürgermeisters dazu berechtigt.

In der Folgezeit versuchte der Verbandsgemeinderat wiederholt neue Beschlüsse zu fassen, durch welche die gesamte Aktion nachträglich eine rechtmäßige Grundlage erhalten sollte. Diese wurden jedoch letztlich alle durch die Kommunalaufsicht bean-

standet. Begründet wurde dies letztendlich damit, dass für den Vollzug der Beschlüsse und die Gestaltung von Rechtsbeziehungen mit Dritten in einer Kommune stets der Bürgermeister zuständig sei. Die Vertretung als Gremium kann diese Aufgabe, auch nicht durch einen Beschluss, an sich ziehen. Das bedeutet, dass die Vertretung keinen Auftrag an die IT-Firma hätte erteilen dürfen. Diese Aufgabe hätte in Zeiten der Abwesenheit des Verbandsgemeindebürgermeisters nur seiner Stellvertreterin zugestanden.

Durch das Handeln des Verbandsgemeinderates haben einige Vertreter dieses Verbandsgemeinderates eine Sammlung personenbezogener Daten in die Hände bekommen, die allein der Verbandsgemeindeverwaltung zugestanden hätte. Der Verbandsgemeinderat erhält nur Kenntnis von personenbezogenen Daten, welche er für Entscheidungen, für die er zuständig ist, benötigt. Aus datenschutzrechtlicher Sicht steht somit fest, dass sich ein nicht namentlich bekannter Personenkreis Zugang zu personenbezogenen Daten verschafft hatte, die er für seine Aufgabenerfüllung nicht benötigte.

Auch die Staatsanwaltschaft ermittelte in diesem Vorgang und stellte die Verfahren gegen Zahlung einer Geldbuße ein. Eine abschließende datenschutzrechtliche Beurteilung auch unter Einbeziehung der Ergebnisse des parallelen Petitionsverfahrens im Landtag von Sachsen-Anhalt steht noch aus.

13.4.3 Auskunftsanspruch der Vertretung der Kommune

Im zurückliegenden Berichtszeitraum häuften sich Anfragen von Kommunen, in welchem Umfang und welche personenbezogenen Daten dem Rat als Vertretung der Kommune durch die Kommunalverwaltung vorgelegt werden müssten.

Dazu ist auf § 10 DSG LSA zu verweisen. Danach ist das Nutzen personenbezogener Daten nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und für die Zwecke erfolgt, für die sie erhoben worden sind. Eine Zweckänderung ist nur nach den besonderen Voraussetzungen des Absatzes 2 zulässig.

Die Aufgaben der Vertretung ergeben sich aus § 45 KVG LSA. Weitere Aufgaben können in der Hauptsatzung festgeschrieben werden.

Sollte eine Aufgabe eindeutig dem Hauptverwaltungsbeamten zugewiesen sein, darf die Vertretung diese Aufgabe nicht an sich ziehen. Jedoch darf jedes Mitglied der Vertretung nach § 45 Abs. 7 KVG LSA über einzelne Angelegenheiten der Kommune und ihrer Verwaltung Auskunft vom Hauptverwaltungsbeamten verlangen (zusätzliche Gruppenrechte in § 45 Abs. 6 KVG LSA).

Hier richtet sich der Informationsanspruch nur auf solche Informationen, die zur Aufgabenerfüllung der Kommunalverwaltung gehören. Ist die Aufgabe auf einen Zweckverband übergegangen, so ist auch das Fragerecht auf die Delegierten für die Zweckverbandsversammlung übergegangen. Das Fragerecht könnte durch spezialgesetzliche Regelungen wie z. B. das Personalaktengeheimnis, das Steuergeheimnis oder das Sozialaktengeheimnis beschränkt sein.

13.4.4 Kampf gegen Hundekot

In vielen Kommunen wird überlegt, auf welche Weise der Ort sauber gehalten werden kann, ohne dass große Kosten entstehen. Besonders unangenehm fallen dabei immer wieder die Hundehalter auf, deren Vierbeiner sich auf den Gehwegen und in den Parks „verewigen“ und deren Hundehaufen unerlaubt einfach liegen gelassen werden.

Ein Ortsbürgermeister hatte eine Idee, wie man Herr der Lage wird. Er rief die Einwohner seines Dorfes auf, jeden Halter zu melden, der seine Hundehaufen einfach liegen lässt. In der Zeit der weit verbreiteten Smartphones sollten doch wenn möglich auch Fotos von den Taten gemacht werden. Mit den Fotos würde der Ortsbürgermeister das Gespräch mit den Hundehaltern suchen, ehe ein Verfahren durch das Ordnungsamt eingeleitet würde.

Ein solcher Aufruf verstößt gegen das allgemeine Persönlichkeitsrecht. Für die Fertigung und die Verbreitung von Fotos gilt das Kunsturhebergesetz (KunstUrhG). Nach § 22 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Hier spricht man auch vom Recht am eigenen Bild.

Somit dürfen Bilder von Personen grundsätzlich nicht ohne Wissen der abgebildeten Person weitergegeben werden. Nach dem KunstUrhG ist es dabei unerheblich, ob damit kommerzielle Zwecke verfolgt werden oder nicht und ob das Bild veröffentlicht werden soll oder nur an eine Einzelperson weitergereicht wird.

Diese Rechtsmeinung wurde bereits mehrfach durch die Rechtsprechung bestätigt. Aktuell hat am 28. Januar 2014 das Amtsgericht Bonn unter Az. 109 C 228/13 bestätigt: *“Die Herstellung eines Bildnisses ohne Einwilligung des Abgebildeten kann einen unzulässigen Eingriff in dessen nach § 823 Abs. 1 BGB geschütztes allgemeines Persönlichkeitsrecht bedeuten. Dabei kann auch die Herstellung von Bildnissen einer Person in öffentlich zugänglichen Bereichen und ohne Verbreitungsabsicht (…) einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen bedeuten.“* Weiter bestätigte das Amtsgericht, dass der Schutzbereich des Rechts am eigenen Bild bereits eröffnet ist, wenn ohne die Einwilligung des Abgebildeten ein Bildnis gefertigt wird. Auf die Absicht einer Verbreitung oder Veröffentlichung kommt es dabei nicht an.

Diese Rechtsauffassung vertrat der Landesbeauftragte auch gegenüber der Stadt. Der behördliche Datenschutzbeauftragte der Stadt kam in seiner datenschutzrechtlichen Bewertung des Vorganges zu demselben Ergebnis, und teilte diese auch dem Ortsbürgermeister mit der Bitte, nicht zum Fotografieren der Hundehalter aufzurufen, mit.

13.4.5 Erlaubnis zur Ausübung des Bewachungsgewerbes

Wer gewerbsmäßig Leben oder Eigentum fremder Personen bewachen will, also das Bewachungsgewerbe auszuüben beabsichtigt, bedarf nach § 34a GewO der Erlaubnis der zuständigen Behörde. Zuständig sind in Sachsen-Anhalt in der Regel die Gemeinden. Personen, die das Bewachungsgewerbe ausüben, sollten zwangsläufig das Vertrauen ihres Auftraggebers, der ihnen zum Teil hohe Sachwerte anvertraut,

genießen und auch rechtfertigen. Die GewO bestimmt aus diesem Grunde klar, welche Voraussetzungen erfüllt werden müssen, um dieses Gewerbe auszuüben. So darf die Erlaubnis z. B. dann nicht erteilt werden, wenn Tatsachen die Annahme rechtfertigen, dass der Antragsteller nicht die für den Gewerbebetrieb erforderliche Zuverlässigkeit besitzt. Unzuverlässigkeit läge nach § 34a Abs. 1 GewO auch vor, wenn der Antragsteller Mitglied eines verbotenen Vereins oder einer verfassungswidrigen Partei ist oder war oder er Bestrebungen gegen die freiheitlich-demokratische Grundordnung verfolgt oder einst verfolgte. Die Erlaubnis wäre auch dann zu versagen, wenn der Antragsteller nicht nachweisen kann, über die für den Gewerbebetrieb erforderlichen Mittel oder entsprechende Sicherheiten zu verfügen.

Verwaltungshandeln und vor allem Verwaltungsentscheidungen sind nachvollziehbar zu dokumentieren und zu begründen. Aus diesem Grunde ist in den Akten der Verwaltungsbehörde über die Erteilung oder Nichterteilung von Erlaubnissen zur Ausübung des Bewachungsgewerbes eine Fülle sensibler personenbezogener Daten gespeichert. Der Landesbeauftragte hatte im Berichtszeitraum solche Akten kontrolliert. Speziell die Dokumentation, dass der Antragsteller die für den Gewerbebetrieb erforderlichen finanziellen Mittel oder entsprechende Sicherheiten nachgewiesen hatte, war dabei von Interesse. Dem Landesbeauftragten war nämlich aus Kontrollen im Sozialbereich bekannt, dass zur Dokumentation der finanziellen Verhältnisse eines Antragstellers durch die Ämter häufig Kontoauszüge – gern von einem längeren Zeitraum – zu den Akten genommen werden, was sich bei der Kontrolle der Bewachungsgewerbeakten teilweise auch bestätigte. Es stellt jedoch einen erheblichen Unterschied dar, ob ein Antragsteller zu einem bestimmten Zeitpunkt über einen gewissen Vermögensbestand verfügt oder ob für einen Bewilligungszeitraum für Sozialleistungen der Saldo seiner relevanten Einnahmen und Ausgaben eine bestimmte Höhe nicht überschreitet. Im ersten Fall muss er also über eine bestimmte Leistungsfähigkeit verfügen, im zweiten Fall darf er es längere Zeit nicht. Genau dieser Unterschied wirkt sich in der Dokumentation der Antragsbearbeitung aus. Während für den einkommensabhängigen Bezug von laufenden Sozialleistungen im Einzelfall durchaus erforderlich sein kann, mehrere fortlaufende Kontoauszüge – ggf. mit Schwärzungen – zur Akte zu nehmen, wird es für die Dokumentation des Vorhandenseins der erforderlichen finanziellen Mittel gemäß § 34a Abs. 1 Satz 3 Nr. 2 GewO genügen, in der Akte zu notieren, dass der Nachweis erfolgte. Dieser könnte durch Vorlage von Kontoauszügen oder Sparkassenbüchern erfolgt sein. Es ist jedoch für die genannte Feststellung der wirtschaftlichen Leistungsfähigkeit überhaupt nicht von Relevanz, dass ein Antragsteller Mitglied in einem Kleintierzüchter- oder Sportverein oder Stammkunde bei einem Versender von Erotikartikeln ist oder nachehelichen Unterhalt in bestimmter Höhe zahlt. Kopien von Bankunterlagen mit solchen Angaben haben in den Erlaubnisakten nach § 34a GewO deshalb nichts zu suchen, da die Speicherung der genannten Daten gegen das Gebot der Datensparsamkeit aus § 1 Abs. 2 DSG LSA verstößt. Bei seinen Kontrollen hatte der Landesbeauftragte die verantwortlichen Stellen, soweit das im Einzelfall erforderlich war, nachdrücklich auf diese Rechtslage hingewiesen. In allen Fällen wurden die Mängel zeitnah beseitigt und die Akten bereinigt.

13.5 Zensus 2011 – Löschung der Daten

Über die Auswertung des Zensus 2011 aus datenschutzrechtlicher Sicht hatte der Landesbeauftragte bereits in seinem XI. Tätigkeitsbericht (Nr. 12.6) sein Resümee

gezogen und auch einen Ausblick auf den möglichen Zensus 2021 gegeben. Gleichwohl zeigte sich im Berichtszeitraum eine Entwicklung, die Anlass gibt, das Thema Zensus noch einmal aufzugreifen. Die Ursache liegt in der Verpflichtung der Statistischen Landesämter nach § 19 ZensG 2011, die Hilfsmerkmale der Zensusdaten von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen, sodann gesondert aufzubewahren und zu löschen, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist, was nach dem Gesetz spätestens am 9. Mai 2015 der Fall sein musste. Die Bekanntgabe der amtlich festgestellten Einwohnerzahlen der Gemeinden durch die amtliche Statistik im Mai 2013 dürfte als Signal zu verstehen gewesen sein, dass die Schlüssigkeits- und Vollständigkeitsprüfung abgeschlossen ist. Dann hätte also mit der Löschung der Hilfsmerkmale begonnen werden müssen.

Mit der Bekanntgabe der Einwohnerzahlen wurden jedoch teils erhebliche Differenzen zu den bisher angenommenen Einwohnerzahlen der Kommunen manifestiert. Ob nun die einst fehlerhaften Einwohnerzahlen durch den Zensus 2011 korrigiert oder die einst richtigen Einwohnerzahlen durch den Zensus fehlerhaft ermittelt wurden, entzieht sich der Beurteilung durch den Landesbeauftragten. Jedenfalls werden die bei vielen Kommunen verringerten Einwohnerzahlen zu einer Verringerung der kommunalen Einnahmen aus dem Finanzausgleich führen. Das wiederum wollten viele Bürgermeister und ihre Kämmerer nicht hinnehmen und erhoben Klage vor den Verwaltungsgerichten, in acht Fällen auch in Sachsen-Anhalt. Vereinfacht dargestellt wurde dort begehrt festzustellen, dass die amtliche Statistik fehlerhaft sei. Naturgemäß kann das jedoch nur unter Vorlage belastbaren und vollständigen Zahlenmaterials aus der amtlichen Statistik, also den kompletten Hilfs- und Erhebungsmerkmalen, gelingen.

Spätestens hier werden die datenschutz- und statistikrechtlichen Probleme deutlich, in denen Verwaltungsrichter, Statistiker und Kommunalbeamte stecken. Einerseits sind die Hilfsmerkmale des Zensus zu löschen, andererseits lässt sich nur durch ihr physisches und vollständiges Vorhandensein ihre Richtigkeit (durch die amtliche Statistik) oder Unrichtigkeit (durch die Kommunen) beweisen. Während sich die amtliche Statistik in einigen Bundesländern dazu entschlossen hatte, die eigentlich fällige Löschung der Hilfsmerkmale im Vorgriff auf möglicherweise später eingehende verwaltungsgerichtliche Auflagen- oder Aufklärungsbeschlüsse oder Anordnungen aufzuschieben, hatte man sich im Statistischen Landesamt Sachsen-Anhalt strikt an das Gesetz gehalten. Das Statistische Landesamt teilte dem Landesbeauftragten im Jahre 2014 mit, die in seinem eigenen Zugriff befindlichen Datenbestände des Zensus 2011 seien bereits gelöscht worden.

Unabhängig davon wären die Verwaltungsgerichte gehindert, die Zensus-2011-Einzeldatensätze zum Gegenstand gerichtlicher Verfahren zu machen. Dem steht nämlich ihre gesetzliche Geheimhaltungspflicht nach § 16 Abs. 1 Satz 1 BStatG entgegen. Eine solche im grundrechtlichen Interesse geschaffene Geheimhaltungspflicht ist auch im gerichtlichen Verfahren zu beachten. Genau das hatte z. B. das Verwaltungsgericht Bremen in seinem Urteil vom 6. November 2014 (Az. 4 K 841/13) festgestellt. Die Daten hätten, so das Gericht, „von vornherein nicht in das gerichtliche Verfahren eingeführt werden können“. Dies bewirkte, dass nicht sämtliche Verfahrensschritte des Zensus 2011 überprüft werden und im Einzelfall möglicherweise gemachte Fehler unerkannt bleiben. Diese Einschränkung findet ihre Rechtfertigung

im Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen. Eingriffe hierin bedürfen einer gesetzlichen Grundlage, die nicht vorhanden sei.

Jedoch hat das Bundesverfassungsgericht in einem einstweiligen Normenkontrollverfahren auf Antrag Berlins § 19 ZensG 2011 außer Vollzug gesetzt. Die effektive Überprüfung der Einwohnerzahlberechnung habe mehr Gewicht als der Eingriff in die informationelle Selbstbestimmung; die Folgenabwägung erlaube eine befristete Weiterspeicherung (BVerfG, Beschluss vom 26. August 2015, Az. 2 BvF 1/15).

14 Wirtschaft

14.1 Düsseldorfer Kreis – Themen und Arbeitsgruppen

Bereits im XI. Tätigkeitsbericht (Nr. 13.1) wurde der Düsseldorfer Kreis als bundesweites Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vorgestellt. Sitzungen finden zweimal jährlich statt, an denen der Landesbeauftragte regelmäßig teilnimmt. Darüber hinaus werden einzelne Themen im schriftlichen Verfahren erörtert. Ziel der Beratungen ist es, die Auffassungen zu grundsätzlichen Themen oder länderübergreifenden Sachverhalten abzustimmen, um zu einer möglichst einheitlichen Auslegung datenschutzrechtlicher Vorschriften und Verwaltungspraxis zu kommen. Neben intensiven Beratungen zu unterschiedlichen Einzelthemen hat der Düsseldorfer Kreis im Berichtszeitraum folgende Beschlüsse gefasst und veröffentlicht:

- Beschluss vom 11. und 12. September 2013: Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

  Intention des Beschlusses ist es, darauf hinzuweisen, dass bei einer Übermittlung personenbezogener Daten in einen Staat außerhalb des Europäischen Wirtschaftsraums (Drittstaat) in einer ersten Prüfungsstufe die allgemeinen Datenschutzvorschriften, die eine Übermittlung erlauben, zu prüfen sind, z. B. § 28 BDSG. Danach sind die Vorschriften zu prüfen, die eine Übermittlung speziell in Drittstaaten ermöglichen (**Anlage 35**; vgl. auch zu Safe Harbor Nr. 3.2.1).

- Beschluss vom 27. Januar 2014: Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten

  Der Beschluss weist darauf hin, dass die Erhebung und Speicherung von personenbezogenen Daten der Mietinteressenten nur dann zulässig ist, wenn dafür ein berechtigtes Interesse besteht oder die Daten für die Durchführung des späteren Mietvertrages erforderlich sind. Die Frage, welche Daten erhoben und gespeichert werden können, hängt insbesondere davon ab, ob lediglich ein Besichtigungstermin vereinbart werden soll, der Mietinteressent bereits erklärt hat, die Wohnung anmieten zu wollen oder der Vermieter sich schon für einen konkreten Interessenten entschieden hat (**Anlage 36**, siehe auch Nr. 14.13).

- Beschluss vom 19. Februar 2014: Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen

Aufgrund ständig zunehmender Videoüberwachungen – insbesondere in öffentlich zugänglichen Räumen – sahen es die Aufsichtsbehörden als erforderlich an, auf die rechtlichen Grenzen hinzuweisen (siehe Nr. 15.2.1). Die Orientierungshilfe ist auf der Homepage des Landesbeauftragten abrufbar.

- Beschluss vom 25. und 26. Februar 2014 zur Unzulässigkeit von Videoüberwachungen aus Fahrzeugen (**Anlage 37**)

  Der Beschluss zeigt auf, dass die Speicherung personenbezogener Daten mithilfe einer sogenannten Dashcam in aller Regel unzulässig ist (siehe Nr. 15.2.7).

- Beschluss vom 25. und 26. Februar 2014: Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

  Mit dem Beschluss will der Düsseldorfer Kreis dazu beitragen, dass verantwortliche Stellen ihre Eigenverantwortung stärken. Dies kann insbesondere dadurch geschehen, Prüfzertifikate im Bereich des Datenschutzes zu entwickeln und die betriebsinternen Verfahrensweisen im Umgang mit personenbezogenen Daten einem Audit zu unterziehen (siehe **Anlage 38**, vgl. auch Nr. 14.2).

- Beschluss vom Mai 2014 (Umlaufbeschluss): Smartes Fernsehen nur mit smartem Datenschutz (**Anlage 39**)

  Smart-TV bieten die Möglichkeit der Nutzung von Internet-Diensten. Dadurch ist es technisch aber auch möglich, das Nutzerverhalten auszuwerten. Der Beschluss beschreibt die datenschutzrechtlichen Anforderungen an Endgerätehersteller, Sender sowie alle weiteren Anbieter von Telemedien (siehe auch Nr. 5.6).

- Beschluss vom 16. Juni 2014: Orientierungshilfe zu den Datenschutzanforderungen an App-Anbieter und App-Entwickler

  Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps) für Smartphones und Tablets im nicht-öffentlichen Bereich, die als Telemediendienst zu qualifizieren sind. Sie beschreibt die datenschutzrechtlichen und technischen Anforderungen. Die Orientierungshilfe ist auf der Homepage des Landesbeauftragten abrufbar.

Der Düsseldorfer Kreis hat eine Reihe von Arbeitsgruppen (AG) eingerichtet, die ein- oder zweimal jährlich tagen. Dort werden Schwerpunktbereiche vertieft behandelt. Wichtig in diesen Arbeitsgruppen ist neben dem Gedankenaustausch unter den Aufsichtsbehörden die Beratung mit Vertretern einzelner Wirtschaftsbranchen. Dadurch wird es z. B. ermöglicht, detailliert den dortigen Umgang mit personenbezogenen Daten einzuschätzen und dem Düsseldorfer Kreis Beschlussentwürfe vorzulegen, zu denen die betroffenen Branchen bereits Gelegenheit zur Stellungnahme hatten. Der Landesbeauftragte hat an folgenden AG teilgenommen: AG Internationaler Daten-

verkehr, AG Sanktionen, AG Auskunfteien, AG Kreditwirtschaft, AG Werbung und Adresshandel, AG Videoüberwachung, Workshop der Aufsichtsbehörden.

Leider lässt es die derzeitige personelle Situation nicht zu, regelmäßig an allen AG-Sitzungen teilzunehmen.

14.2 Datenschutzmanagement

Der Landesbeauftragte hat eine Broschüre für kleine und mittelständische Unternehmen unter dem Titel **„Datenschutz ist Chefsache“** herausgegeben. Wie der Titel deutlich macht, wendet sie sich an Unternehmensleitungen und deren Management. Sie enthält grundlegende Hinweise zum Datenschutz. Sie soll als Orientierungshilfe bei der Durchführung notwendiger Maßnahmen zur Umsetzung von Datenschutz und Datensicherheit sowie als Leitfaden zur Selbstprüfung dienen. Sie kann in ausgedruckter Version per Briefpost oder E-Mail bestellt werden. Zudem steht sie online zum Abruf zur Verfügung[10].

In der Broschüre, aber auch bereits im XI. Tätigkeitsbericht (Nr. 4.6), wurde der Datenschutz als Führungsaufgabe qualifiziert. Daher ist im Falle von anlassabhängigen oder anlasslosen Kontrollen nach § 38 BDSG für den Landesbeauftragten immer die Unternehmensleitung als Vertretung der verantwortlichen Stelle nach § 3 Abs. 7 BDSG Ansprechpartner. Dies gilt auch dann, wenn im Einzelfall eine individuelle datenschutzrechtliche Verfehlung eines Mitarbeiters vorliegen sollte. Auch hier stellt sich die Frage, ob die Leitung und das Management des Unternehmens seiner Aufgabe, die betriebsinternen Prozesse entsprechend den Anforderungen zu planen, zu organisieren, zu steuern und zu kontrollieren, nachgekommen ist.

Angesichts der im Berichtszeitraum durchgeführten Kontrollen ergaben sich im Wesentlichen folgende Fragenkomplexe, die aus Sicht des Landesbeauftragten dem Management eines Unternehmens bzw. direkt der Unternehmensleitung zu stellen sind:

1. Welche personenbezogenen Daten werden erhoben, verarbeitet oder genutzt? Werden besondere Arten von personenbezogenen Daten erhoben, verarbeitet oder genutzt (hier wären die Einschränkungen von § 28 Abs. 6 bis 9 zu beachten)? Welche Personengruppen sind betroffen (Kunden, Lieferanten, weitere Geschäftspartner, Beschäftigte, Beworbene)?

2. Werden die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet und personenbezogene Daten nur entsprechend dem Zweck der Erhebung verarbeitet oder genutzt? Werden Daten rechtzeitig gelöscht? Werden Daten, die nicht gelöscht werden dürfen (z. B. wegen § 257 HGB), gemäß § 35 Abs. 3 BDSG gesperrt?

3. Sind Zuständigkeiten und Kompetenzen bezüglich des Umgangs mit personenbezogenen Daten eindeutig festgelegt und dokumentiert? Ist für die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten die Zustimmung des Betriebsrates erforderlich? Sind die bei der Datenverarbeitung Beschäftig-

[10] http://lsaurl.de/chefsache

ten dafür ausreichend geschult und gemäß § 5 BDSG auf das Datengeheimnis verpflichtet?

4. Sind die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen umgesetzt? Findet eine Überprüfung statt, wenn neue Technik eingesetzt wird? Gibt es Rollen- und Zugriffskonzepte, die den Zugriff Unberechtigter auf personenbezogene Daten ausschließen? Sind bei Internetanschlüssen aktuelle Firewall und aktueller Virenschutz vorhanden? Werden mobile Datenträger sicher verschlüsselt?

5. Werden bei Nutzung der Unternehmenswebseite personenbezogene Daten erhoben und gespeichert? Wenn ja, wurde die Zulässigkeit überprüft? Ist eine Datenschutzerklärung vorhanden, die gemäß § 13 TMG über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten informiert (z. B. bei Verwendung von Cookies oder Webanalysetools)?

6. Wurden externe Unternehmen mit der Datenverarbeitung betraut, z. B. im Rahmen des Cloud-Computing oder eines Auftrags zur Datenträgervernichtung? Wurden externe Unternehmen mit Wartungsarbeiten von Datenverarbeitungsunterlagen beauftragt? Wenn eine der Fragen mit „ja“ zu beantworten ist: Wurde ein Vertrag über eine Auftragsdatenverarbeitung gemäß § 11 BDSG abgeschlossen? Wird der Auftragnehmer regelmäßig bezüglich der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen kontrolliert?

7. Sind im Unternehmen mindestens zehn Beschäftigte mit der automatisierten Verarbeitung oder mindestens 20 Personen mit der manuellen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt? Unterliegt eine der Verarbeitungen der Vorabkontrolle nach § 4d Abs. 5 BDSG? Wenn eine dieser Varianten vorliegt: Wurde ein betrieblicher Datenschutzbeauftragter bestellt? Wenn ja, ist er ausreichend geschult? Führt er für Verfahren automatisierter Verarbeitungen das erforderliche Verfahrensverzeichnis?

8. Falls personenbezogene Daten an Dritte übermittelt werden: Wurde die Zulässigkeit dieser Übermittlung geprüft?

9. Ist sichergestellt, dass erforderliche Meldungen nach den §§ 4d und 42a BDSG an die Datenschutzaufsichtsbehörde erfolgen?

10. Können alle auftretenden Fragen mit eigenem Fachwissen beantwortet werden oder wird externe Beratung bzw. Unterstützung benötigt? Sollte das betriebliche Datenschutzmanagement mithilfe eines Audits überprüft werden? Bestehen Kontakte zur Datenschutzaufsichtsbehörde?

Sicherlich muss die Unternehmensleitung nicht alle dieser Fragen bis ins Detail selbst beantworten. Jedoch tauchen viele dieser Fragen in den meisten Unternehmen auf. Die Leitung muss daher zur Vermeidung eines Organisationsverschuldens veranlassen, dass die konkret auftretenden Fragen geklärt werden und ein rechtmäßiger Umgang mit personenbezogenen Daten gewährleistet ist.

14.3 Meldepflichten bei Datenpannen

Gemäß **§ 42a BDSG** sind verantwortliche Stellen in bestimmten Fällen verpflichtet, Betroffene sowie den Landesbeauftragten zu benachrichtigen. Voraussetzung für diese Benachrichtigungspflichten ist zunächst, dass nach § 42a Abs. 1

- besondere Arten personenbezogener Daten (Nr. 1),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen (Nr. 2),
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder entsprechende Verdachtsmomente beziehen (Nr. 3)
- oder personenbezogene Daten zu Bank- oder Kreditkartenkonten (Nr. 4)

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind (sog. Datenpannen). Weitere Voraussetzung für die Benachrichtigungspflichten ist, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der Betroffenen drohen. Anders als der Wortlaut dieser Vorschrift zu implizieren scheint, bestehen die Benachrichtigungspflichten schon dann, wenn aus Sicht der verantwortlichen Stelle eine hohe Wahrscheinlichkeit für die Kenntnisnahme durch Dritte besteht (vgl. Gola, BDSG Kommentar, 12. Auflage, § 42a Rn 4).

So war es folgerichtig, dass ein Kreditinstitut einen Vorfall meldete, bei dem etliche Kontounterlagen mit Namen, Kontonummern, Adressen und Salden von einer Reinigungskraft, die offenbar nur vertretungsweise tätig wurde, in einen öffentlich zugänglichen Papiercontainer geworfen wurden. Da dieser Umstand nach kurzer Zeit festgestellt, und ein Mitarbeiter des Instituts die Unterlagen sofort wieder an sich nahm, war nicht mit Sicherheit anzunehmen, dass Dritte davon Kenntnis erlangten (siehe auch Nr. 14.9).

Im Berichtszeitraum wurde der Landesbeauftragte in einem anderen Fall mit dem Argument eines Geldinstituts konfrontiert, dass bei einer erfolgten unrechtmäßigen Übermittlung von Kontodaten keine schwerwiegenden Beeinträchtigungen zu befürchten seien, da das Institut eventuelle Abbuchungen durch Rückbuchungen ersetzen würde. Widerspruchs- oder Rückbuchungsmöglichkeiten sollten bei der Beurteilung der schwerwiegenden Beeinträchtigungen jedoch außer Betracht bleiben. Denn auch die Notwendigkeit, einer zu Unrecht erfolgten Belastung des Kontos rechtzeitig widersprechen zu müssen, ist bereits eine Beeinträchtigung der Interessen des Betroffenen (Dix, in: Simitis, BDSG, 8. Auflage, § 42a Rn. 9). Daher sollten Meldungen auch erfolgen, wenn die verantwortliche Stelle bereit ist, eventuell auftretende Schäden zu ersetzen.

In einer weiteren Meldung wurde dem Landesbeauftragten mitgeteilt, dass eine zuvor gekündigte Mitarbeiterin einer großen Versicherung Listenausdrucke von Kundendaten an einen konkurrierenden Versicherungsvertreter übergeben hat, der die Tat letztendlich der Versicherung meldete. Enthalten waren Namen, Anschriften, Telefonnummern, umfangreiche Daten zu bestehenden Versicherungen, Wagnisdaten und Bankverbindungen. Nach Beendigung des Beschäftigungsverhältnisses bestand natürlich kein Grund für die Mitarbeiterin, diese Unterlagen noch zu besitzen. Sie hätte die Unterlagen ihrem ehemaligen Arbeitgeber übergeben oder vernichten müssen. Durch die Übergabe der Unterlagen an den konkurrierenden Versicherungsvertreter besteht für den Landesbeauftragten sogar der Verdacht einer Straftat nach § 44 Abs. 1 BDSG. Nach dieser Vorschrift wird bestraft, wer unbefugt personenbezogene

Daten, die nicht allgemein zugänglich sind, einem Dritten übermittelt und dabei mit Bereicherungsabsicht handelt. Auf die Frage, ob der Versicherungsvertreter die Unterlagen tatsächlich eingesehen hat, kommt es hier nicht an. Ein „Übermitteln“ personenbezogener Daten liegt bereits dann vor, wenn sie einem Dritten durch Weitergabe bekanntgegeben werden. Dies ist bereits erfüllt, wenn der Empfänger die Möglichkeit hat, ungehindert die Informationen zur Kenntnis zu nehmen (Dammann, in Simitis, a. a. O. § 3 Rn. 146). Aufgrund der Weitergabe der Unterlagen ausgerechnet an einen Versicherungsvertreter liegen auch zureichende tatsächliche Anhaltspunkte für die Absicht vor, dass die gekündigte Mitarbeiterin sich selbst bereichern wollte. Der Landesbeauftragte hat daher nach § 44 Abs. 2 BDSG Strafantrag bei der zuständigen Staatsanwaltschaft gestellt. Das Verfahren ist dort noch anhängig.

Nicht alle eingegangenen Meldungen zu § 42a BDSG wurden vom Landesbeauftragten so eingeschätzt, dass tatsächlich eine Benachrichtigungspflicht bestand. Dies lag insbesondere daran, dass mitunter nach Prüfung des Einzelfalles festgestellt wurde, dass keine schwerwiegenden Beeinträchtigungen drohten. Gleichwohl rät der Landesbeauftragte, ihn auch in Zweifelsfällen zu informieren. Das Risiko einer fehlerhaften Prognose trägt die verantwortliche Stelle. Unterbleibt eine erforderliche Benachrichtigung oder ist sie nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgt, so liegt im Falle von Vorsatz oder Fahrlässigkeit eine Ordnungswidrigkeit vor, die mit einer Geldbuße bis zu 300.000 € geahndet werden kann.

Zu den weiteren Handlungspflichten der verantwortlichen Stellen im Zusammenhang mit Datenpannen vgl. Nr. 13.1.2 des XI. Tätigkeitsberichts mit weiteren Quellenangaben.

14.4 Geoinformation

GeoBusiness-Verhaltenskodex „GeoBusiness und Datenschutz“

Bereits seit Jahren hat sich in der Wirtschaft die Erkenntnis durchgesetzt, dass in der gewerblichen Nutzung der im Rahmen des Open Government bereitgestellten staatlichen Geoinformationen ein erhebliches Wertschöpfungspotential steckt. Zur Sicherung der rechtmäßigen Nutzung dieses Potentials ist es sinnvoll, wenn die die Geodaten verarbeitende Wirtschaft eine Selbstverpflichtung nach § 38a BDSG abgeben würde. Solche „Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen“ sollten unter maßgeblicher Mitwirkung einer von der GIW-Kommission ins Leben gerufenen TaskForce „GeoBusiness Datenschutz“, in der auch der Landesbeauftragte beteiligt ist, erarbeitet werden. In seinem XI. Tätigkeitsbericht (Nr. 13.1.3) hatte der Landesbeauftragte über Arbeit und Ziele der TaskForce bereits umfänglich berichtet.

Der GeoBusiness-Verhaltenskodex (CoC) verfolgt folgende Ziele:

- Schaffung eines rechtssicheren, einfachen und standardisierten Zugangs der Wirtschaft zu staatlichen Geodaten,
- Konkretisierung der einschlägigen datenschutzrechtlichen Vorschriften und Bereitstellung von entsprechenden Auslegungs- und Anwendungshinweisen,
- Erleichterung des Entscheidungsprozesses der Geodaten haltenden öffentlichen Stellen, welche Geodaten in welcher Form an die Wirtschaft herausgegeben werden können,

- Selbstverpflichtung der Wirtschaft zum datenschutzgerechten Umgang mit Geodaten und damit die
- Stärkung der Eigenverantwortung der Wirtschaft.

Das Ziel der TaskForce war, den CoC zunächst vom Düsseldorfer Kreis bestätigen zu lassen, um ihn dann im förmlichen Verfahren nach § 38a BDSG einer Aufsichtsbehörde zu unterbreiten. Soweit kam es jedoch zunächst nicht. Der Entwurf des CoC war wegen fehlender Beschlussreife durch den Düsseldorfer Kreis an die TaskForce zurückgegeben worden. Der Auftrag war, die wohl auch dem Föderalismus geschuldeten unterschiedlichen Sichtweisen der Landesbeauftragten, hervorgerufen durch unterschiedliche landesrechtliche Vorschriften, z. B. zum Geodatenzugang, zu vereinheitlichen und den CoC damit universell zu machen. Die Arbeit an diesem Auftrag fand im Jahre 2015 ihr vorläufiges Ende. Der Düsseldorfer Kreis verständigte sich auf seiner Sitzung im März 2015 darauf, den CoC anzunehmen. Damit war der Weg frei, ihn i. S. von § 38a Abs. 1 BDSG förmlich der zuständigen Aufsichtsbehörde zu unterbreiten und diese um Überprüfung zu ersuchen. Dies ist im Juli 2015 durch den Berliner Datenschutzbeauftragten erfolgt.

Datenschutzkodex für Geodatendienste

Der Datenschutzkodex für Geodatendienste der BITKOM aus dem Jahre 2010, nicht zu verwechseln mit dem oben beschriebenen GeoBusiness CoC, war mit dem Ziel erarbeitet worden, die Akzeptanz der breiten Öffentlichkeit für die damals neuartigen Geodatendienste, nämlich die Panoramadienste wie Google Street View, und gleichzeitig die informationelle Selbstbestimmung der Nutzer zu befördern. Darüber, dass diese selbstverpflichtenden Verhaltensregeln im Sinne von § 38a BDSG nicht die breite Zustimmung der Datenschutzaufsichtsbehörden erhielten, und über die Hintergründe, hatte der Landesbeauftragte in seinem X. Tätigkeitsbericht (Nr. 3.1.3) bereits umfassend berichtet. Die Liste der damaligen Kritikpunkte war lang:

- Der Datenschutzkodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung der Betroffenen verletzt. Es fehlt die Möglichkeit des Vorabwiderspruches.
- Viele Veröffentlichungsarten, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft.
- Der Datenschutzkodex ist nur für die Unternehmen bindend, die ihn unterzeichnet haben.

In diesem Zusammenhang wird auf den entsprechenden Beschluss des Düsseldorfer Kreises vom 8. April 2011 „Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert“ verwiesen, der im X. Tätigkeitsbericht als Anlage 28 enthalten ist.

Ebenso wie um die damalige Forderung des Düsseldorfer Kreises, dass nunmehr der Gesetzgeber gefordert sei, wurde es um den ganzen Datenschutzkodex für Geodatendienste in den Folgejahren still. Im Oktober 2014 legte die PwC ihren im Auftrag des Selbstregulierung Informationswirtschaft e. V. (SRIW) erstellten Evaluierungsbe-

richt über den Datenschutzkodex vor. Erwartungsgemäß wurden darin auch die bekannten datenschutzrechtlichen Mängel diskutiert: Auch der fehlende Vorabwiderspruch. Daraufhin wurde durch den SRIW eine überarbeitete Fassung des Datenschutzkodex vorgelegt. Weiterhin wird den Berechtigten darin „ab Bereitstellung des Bildmaterials zum Abruf über das Internet für die Öffentlichkeit“ die unbefristete Möglichkeit eingeräumt, die Unkenntlichmachung ihres Hauses ganz oder teilweise zu verlangen. Leider eben erst „ab Bereitstellung“. Die Diskussion mit dem SRIW hält an.

14.5 Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie.

In seinem XI. Tätigkeitsbericht (Nr. 13.2.1) hatte der Landesbeauftragte umfassend über die datenschutzrechtlichen Anforderungen bei der Einführung von intelligenten Zählern (Smart Meter) bzw. Energienetzen (Smart Grids) informiert und hier insbesondere über die zu diesem Thema verabschiedete Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012 (vgl. XI. Tätigkeitsbericht, Anlage 14) und die damit gleichzeitig veröffentlichte „Orientierungshilfe datenschutzgerechtes Smart Metering“ berichtet. Diese Orientierungshilfe enthält Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering. Wesentlicher Bestandteil der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung von Anwendungsfällen, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Mit der Novellierung des Energiewirtschaftsgesetzes (EnWG) vom 26. Juli 2011 (BGBl. I S. 1554) wurden durch den Bundesgesetzgeber die rechtlichen Rahmenbedingungen für die Datenverarbeitung beim Smart Metering geschaffen. Das Gesetz enthält die erforderlichen grundsätzlichen Datenschutzregelungen. So wird in § 21g EnWG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Messstellenbetreiber, Netzbetreiber und Lieferanten geregelt, welche damit als zum Datenumgang berechtigte Stellen für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich sind. Der Schutzbedarf der personenbezogenen Daten ist abhängig davon, inwieweit aus den Daten Rückschlüsse auf das Verhalten und die Lebensgewohnheiten der Endverbraucher möglich sind.

Näheres sollte nach § 21g Abs. 6 EnWG in einer Rechtsverordnung gem. § 21i EnWG geregelt werden. Diese sollte die in § 21g EnWG festgelegten Grundsätze zum Datenschutz weiter konkretisieren und detailliert ausgestalten. Doch mit dem Gesetzentwurf zur Digitalisierung der Energiewende (BR-Drs. 543/15) wird dieser Weg nicht weiter beschritten, sondern im sogenannten Messstellenbetriebsgesetz (Art. 4 jenes Entwurfs) werden umfängliche Regelungen zur Datensicherheit der Messsysteme getroffen.

14.6 Personalausweiskopie

Der Landesbeauftragte hatte bereits im XI. Tätigkeitsbericht (Nr. 13.2.2) darauf hingewiesen, dass es auch in der Wirtschaft gang und gäbe ist, Personalausweise zu kopieren, obwohl dies regelmäßig nicht erforderlich und damit datenschutzrechtlich unzulässig ist.

Im Berichtszeitraum ist der Landesbeauftragte in seiner Auffassung durch ein sehr deutliches Urteil des VG Hannover vom 28. November 2013 (ZD 2014, 266) bestärkt worden. Darin heißt es u. a.:

„Das Einscannen der Personalausweise von LKW-Fahrern durch einen Logistikdienstleister ist rechtlich unzulässig, und zwar unabhängig von einem etwaigen Einverständnis. Die Normen des Personalausweisgesetzes lassen als bereichsspezifische Datenschutzvorschriften keinen Raum für eine vorrangige oder auch nur ergänzende Heranziehung der Regelungen des Bundesdatenschutzgesetzes."

14.7 Gaststättengesetz des Landes Sachsen-Anhalt

Die Befugnis, das Gaststättenrecht zu regeln, lag bis zum 31. August 2006 im Rahmen der konkurrierenden Gesetzgebung beim Bund. Das änderte sich im Zusammenhang mit der Föderalismusreform zum 1. September 2006. Nach Art. 74 Abs. 1 Nr. 11 GG wurde das Gaststättenrecht aus dem Bereich der konkurrierenden Gesetzgebung herausgelöst und ging auf die Länder über. Solange dort jedoch kein entsprechendes Recht besteht, gilt das (Bundes-)Gaststättengesetz weiter.

Im Oktober 2013 beschloss das Landeskabinett den Entwurf eines Gaststättengesetzes, was der Landesbeauftragte erstmals aus einer Pressemitteilung der Landesregierung erfuhr. Der Pressemitteilung war auch zu entnehmen, dass der Gesetzentwurf bereits mit der IHK, der DEHOGA und den kommunalen Spitzenverbänden umfangreich erörtert worden sei. Ziel des Gesetzes sei die Abkehr vom bisherigen bundesgesetzlich geregelten Erlaubnisverfahren für die Schankerlaubnis hin zu einem personenbezogenen Anzeigeverfahren, was zu einem Bürokratieabbau im Gaststättengewerbe führen soll. Außerdem wolle man den mit dem Alkoholausschank verbundenen Gefahren begegnen und gleichzeitig zu einer Harmonisierung der Rechtslage im mitteldeutschen Wirtschaftsraum beitragen.

Nun ist das Recht der Gaststätten nicht das zentrale Aufgabengebiet des Landesbeauftragten. Umso erstaunter war er darüber, dass der wenige Tage später in den parlamentarischen Raum eingebrachte Entwurf eines Gaststättengesetzes (LT-Drs. 6/2547) auch umfangreiche Verarbeitungen personenbezogener Daten regeln sollte. Hätte die Landesregierung § 40 Satz 2 ihrer eigenen Gemeinsamen Geschäftsordnung der Ministerien und sogar § 14 Abs. 1 Satz 2 DSG LSA beachtet und pflichtgemäß den Landesbeauftragten beteiligt, weil eben im Gesetzentwurf die Verarbeitung personenbezogener Daten geregelt werden sollte, wäre ihr datenschutzrechtliche Kritik erspart geblieben. In der durch den Ausschuss für Wissenschaft und Wirtschaft des Landtages durchgeführten öffentlichen Anhörung zum Gesetzentwurf hatte der Landesbeauftragte erstmalig Gelegenheit, Stellung zu beziehen. Hauptzweck und zentrale Stoßrichtung des Gesetzentwurfes sei, so war dessen Begründung zu entnehmen, den mit dem Alkoholausschank verbundenen Gefahren zu begegnen. Dem Gesetzestext konnte jedoch auch das Ziel entnommen werden, möglicher Schwarz-

gastronomie durch Vereine entgegenzuwirken. Nach § 4 des Gesetzentwurfes musste man sich das zukünftige Verfahren so vorstellen: Entweder betreibt der Verein ein Gastgewerbe mit allen für eine Gastwirtschaft geltenden Verpflichtungen und Beschränkungen und kann Getränke an jedermann abgeben oder er betreibt kein Gastgewerbe. Dann dürfte er seine Getränke nur noch an die eigenen Mitglieder ausschenken. Damit dies von der zuständigen Behörde auch überprüft werden kann, hätte es nach dem Gesetzentwurf für die Vereinsmitglieder nicht etwa genügt, dem Kontrollbeamten den Mitgliedsausweis vorzuzeigen. Vielmehr sollte die Kontrolle anhand eines Mitgliederverzeichnisses erfolgen.

Eine solche Vorschrift wäre nicht nur datenschutzrechtlich bedenklich: Zunächst enthält das Mitgliederverzeichnis die Namen und bei größeren Vereinen wegen möglicher Namensgleichheiten weitere Identifikationsmerkmale, wie Geburtsdatum und Adresse aller Vereinsmitglieder. Zu diesen Mitgliedern, z. B. eines Fußballvereins, zählen auch die jüngsten Nachwuchsspieler. Die zuständige Behörde erhält das Verzeichnis auf Vorrat – verfassungsrechtlich bedenklich und wohl auch ein Verstoß gegen das Gebot der Datensparsamkeit aus § 1 Abs. 2 DSG LSA. Wirklichkeitsfremd wäre außerdem gewesen, dass der Fußballverein quasi in der „dritten Halbzeit“ sein Bier nur an die eigenen Mitglieder abgeben darf, nicht aber an die Spieler der Gastmannschaft, nicht an den Schiedsrichter, nicht an den Pressevertreter und auch nicht an den anwesenden Lokalpolitiker. Wie der Gesetzgeber damit seine Zielstellung, Alkoholmissbrauch zu verhindern, umsetzen wollte, blieb unklar.

Durch die Anforderung eines Mitgliederverzeichnisses durch die zuständige Behörde, aber auch durch eine Fülle von Übermittlungsregelungen im Gesetzentwurf, nach denen die Daten aus der Gewerbeanzeige auch an die zuständige Bauaufsichtsbehörde und die für die Lebensmittelüberwachung, den Gesundheitsschutz und den Jugendschutz zuständigen Behörden sowie bei vorübergehenden Veranstaltungen aus besonderem Anlass auch noch an die zuständigen Finanzbehörden übermittelt werden sollen, wird das Grundrecht auf informationelle Selbstbestimmung bzw. der Schutz personenbezogener Daten im Sinne von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und Art. 6 Abs. 1 Satz 1 der Verfassung des Landes Sachsen-Anhalt eingeschränkt. Diese Grundrechtseinschränkung hätte, wie es Art. 19 Abs. 1 Satz 2 GG verlangt, enumerativ im Gesetz vermerkt bzw. zitiert werden müssen. Dies war jedoch nicht der Fall. Damit war der vorgelegte Gesetzentwurf verfassungswidrig.

Der Gesetzentwurf wurde nachfolgend in verschiedenen Landtagsausschüssen beraten, korrigiert und letztendlich ohne die bedenklichen Vorschriften über die Vereinsmitgliederlisten, dafür aber mit den erforderlichen Hinweisen auf die normierten Grundrechtseinschränkungen beschlossen (Gesetz vom 7. August 2014, GVBl. LSA S. 386).

14.8 Versicherungswirtschaft

Gleich zu Beginn des Berichtszeitraumes wandte sich der betriebliche Datenschutzbeauftragte eines großen Versicherungskonzerns an den Landesbeauftragten. Eine Zusammenarbeit der Versicherung mit einem Kreditinstitut bei der Betreuung von dessen Kunden sollte möglichst datenschutzgerecht gestaltet werden. Konkret ging es um die Frage, ob ein Kreditinstitut den bestehenden Versicherungsschutz seiner

Kunden bei einer Versicherung erfragen darf, um ein auf deren persönliche Bedürfnisse zugeschnittenes Finanzangebot machen zu können.

Eine gesetzliche Vorschrift, die für diesen Fall eine entsprechende Datenerhebung der Bank sowie eine Datenübermittlung von der Versicherung an die Bank vorsieht, existiert nicht. Daher kam als Grundlage dafür nur die Einwilligung des Kunden nach § 4a BDSG in Betracht. Der Landesbeauftragte wirkte insbesondere darauf hin, dass alle Einzeldaten, die an die Bank übermittelt werden sollten, in der Einwilligungserklärung konkret benannt werden, damit der Bankkunde auch genau informiert ist, über welche seiner Daten zukünftig die Bank verfügt. Die Übermittlung von Gesundheitsdaten wurde ausgeschlossen.

14.9 Kreditwirtschaft

Entsorgung von Kontounterlagen im Altpapiercontainer

Personenbezogene Daten zu Bank- und Kreditkartenkonten gehören zwar nicht zu den besonderen Arten personenbezogener Daten, werden aber von Kunden der Kreditwirtschaft als sehr schützenswert angesehen. Dies ist auch nicht verwunderlich, denn wer offenbart schon gerne seine Guthaben – mehr noch seine finanziellen Verpflichtungen – im Detail gegenüber unberechtigten Dritten. Der Gesetzgeber hat daher personenbezogene Daten zu Bank- und Kreditkartenkonten insoweit besonders geschützt, als er für den Fall, dass diese unrechtmäßig Dritten zur Kenntnis gelangen und schwerwiegende Nachteile drohen, gemäß § 42a BDSG Mitteilungspflichten an Betroffene und Aufsichtsbehörden vorgesehen hat.

Ein Kreditinstitut wollte dieser Mitteilungspflicht nachkommen und teilte dem Landesbeauftragten mit, dass irrtümlicherweise diverse Unterlagen mit Kundennamen, deren Kontonummern und Salden von einer Reinigungskraft in einem öffentlich zugänglichen Altpapiercontainer entsorgt wurden. Betroffen seien ca. zwei Dutzend Kunden. Die Reinigungskraft war in der Bank als Vertretung für ihre Kollegin tätig. Es war für die Bank nicht auszuschließen, dass Unberechtigte die Unterlagen zu Kenntnis genommen haben und schwerwiegende Beeinträchtigungen für die betroffenen Kunden drohen könnten (siehe auch Nr. 14.3).

Bei der Entsorgung von Datenträgern mit personenbezogenen Daten – dazu gehören auch Schriftstücke wie z. B. Kontoauszüge – ist äußerste Sorgfalt geboten. Die Entsorgung leitet die Löschung der darauf befindlichen Daten ein. Personenbezogene Daten sind u. a. zu löschen, wenn sie gemäß § 35 Abs. 2 Nr. 3 BDSG für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich sind. Personenbezogene Daten sind aber nur dann als gelöscht zu betrachten, wenn sie gemäß § 3 Abs. 4 Nr. 5 BDSG unkenntlich gemacht sind. Text muss unlesbar sein. Davon kann natürlich bei einer Entsorgung in einem öffentlich zugänglichen Altpapiercontainer nicht die Rede sein. Bei Schriftstücken besteht hier natürlich die Gefahr, dass zumindest diejenigen, die selber ihr Altpapier entsorgen wollen, deren Inhalte zur Kenntnis nehmen.

Die generelle innerbetriebliche Verfahrensweise bei der Entsorgung von Schriftstücken in der betreffenden Bank war zunächst nicht zu beanstanden. Die täglich anfallenden Papierabfälle waren in einem Sack zu sammeln, in einem verschießbaren Raum zu lagern, um anschließend vom Hausmeister geschreddert zu werden

(Grundlage für die Vernichtung von Datenträgern ist seit Oktober 2012 die DIN 66399, siehe XI. Tätigkeitsbericht, Nr. 4.8). Das Problem war nur, dass sich die neue Reinigungskraft, die sich offenbar in einer Stresssituation befand, dieser Regelung nicht bewusst war und somit die Papierabfälle ungeschreddert in den Altpapiercontainer warf. Hier war das innerbetriebliche Datenschutzmanagement gefragt. Die betreffende Bank sicherte zu, dass die Reinigungskräfte – auch die, die nur vertretungsweise tätig werden – erneut über die Altpapierentsorgung belehrt und die Belehrungen jährlich wiederholt werden. In der Folge werden sich die Reinigungskräfte auch in Stresssituationen im Klaren darüber sein müssen, dass zu entsorgende Kontounterlagen nur in dafür vorgesehene Vorrichtungen gehören. Glück im Unglück für die betreffende Bank: schon nach einer Stunde machte ein ehrlicher Nutzer des Altpapiercontainers auf die sachwidrige Entsorgung aufmerksam, woraufhin die Bank die Unterlagen sofort wieder an sich nahm.

Versand von Kontounterlagen an Unberechtigte

Mehrfach gingen beim Landesbeauftragten Beschwerden ein, weil Kunden nicht ihre eigenen Kontounterlagen, sondern die anderer Bankkunden per Briefpost erhielten. In einem Fall wurde sogar eine Zahlungsaufforderung mit diversen Kreditunterlagen an den falschen Adressaten versandt. Die Empfänger, die mitunter das Adressfeld nicht sorgsam lesen, öffnen die Schreiben und nehmen somit unberechtigterweise von personenbezogenen Bankdaten Dritter Kenntnis.

Die „Schuldigen“ derartiger fehlerhafter Versendungen sind schnell ausgemacht. Häufig sind es die Beschäftigten, die aufgrund von Unachtsamkeit die Briefumschläge mit einem falschen Adressaten versehen. So war die Beschäftigte eines Sekretariats damit beauftragt, mehrere maschinell erstellte Schreiben an den gleichen Empfänger zusammen zu versenden, glich aber im Falle der o. g. Zahlungsaufforderung nur die Nachnamen ab. Ein Kunde erhielt daher eigene Kontounterlagen sowie die an einen anderen Kunden mit gleichem Nachnamen gerichtete Zahlungsaufforderung. Der nicht berechtigte Empfänger, der zunächst auf der Zahlungsaufforderung nur seinen Nachnamen zur Kenntnis nahm, öffnete den Briefumschlag und betrachtete diese daher zunächst an ihn gerichtet. Beschäftigten der Kreditwirtschaft ist daher dringend zu raten, vor der Versendung die jeweiligen Kontounterlagen einzeln mit den gesamten Adressaten zu vergleichen.

Fehlerhafte Versendungen stellen – gerade wenn sie mehrfach geschehen – aber auch eine Herausforderung für das Datenschutzmanagement dar. Verantwortliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten, § 9 Satz 1 BDSG. „Erforderlich“ in Sinne dieser Vorschrift sind nach Auffassung des Landesbeauftragten Maßnahmen auch dann, wenn Fehler beim Versand aufgrund des Verschuldens der eigenen Beschäftigten geschehen, mit diesen aber zu rechnen ist. So war es im hier zu beurteilenden Fall. Fehler bei der Zuordnung von Schriftstücken namensgleicher Kunden sind nicht gänzlich auszuschließen. Die verantwortliche Stelle muss daher alle zumutbaren Maßnahmen treffen, um derartige Fehlversendungen zu verhindern. Das Kreditinstitut, welches die Versendung der o. g. Zahlungsaufforderung veranlasste, sicherte dem Landesbeauftragten zu, das Verfahren, welches zum Versand an den falschen Adressaten führte, abzustellen.

Der Versand von Kontounterlagen an Unberechtigte wie auch die unsachgemäße Entsorgung können neben aufsichtsrechtlichen Maßnahmen nach § 38 BDSG (siehe dazu Nr. 1.2) auch zur Einleitung von Ordnungswidrigkeitenverfahren führen (wie auch mehrfach geschehen). Kontodaten sind regelmäßig personenbezogene Daten, die nicht allgemein zugänglich sind. Die unbefugte Übermittlung dieser Daten kann nach § 43 Abs. 2 Nr. 1 BDSG mit einem Bußgeld bis zu 300.000 € geahndet werden.

14.10 Auskunfteien

Aus einem anderen Bundesland erreichte den Landesbeauftragten im Berichtszeitraum eine klarstellende Gerichtsentscheidung, wonach Auskunfteien darauf zu achten haben, dass die über Betroffene zu erteilenden Auskünfte bei gesperrten Daten identisch mit Auskünften sind, die im Fall von nicht vorhandenen Daten erteilt werden (Hessischer Verwaltungsgerichtshof, Beschluss vom 2. Januar 2014, Az. 10 B 1397/13, juris). Das Gericht begründet dies mit dem Willen des Gesetzgebers, der mit der Bestimmung in § 35 Abs. 4a BDSG offensichtlich habe sicherstellen wollen, dass in der Außenwirkung für den Betroffenen, auf den sich die personenbezogenen Daten beziehen, die Sperrung dieselbe Wirkung entfaltet wie eine Löschung. Bei gesperrten Daten ist Dritten daher entweder keine Auskunft, oder ausschließlich die Auskunft zu erteilen, dass zu den betroffenen Datenarten keine Daten gespeichert sind.

Dies entspricht der Rechtsauffassung des Landesbeauftragten, der die in Sachsen-Anhalt tätigen Auskunfteien angeschrieben und auf die Gerichtsentscheidung hingewiesen hat, mit der Folge, dass Mitteilungen wie: *„Eine Auskunfterteilung ist zurzeit nicht möglich/ist zurzeit aus Rechtsgründen nicht möglich“* datenschutzrechtlich nicht (mehr) zulässig sind.

Aufgrund der wenig aussagekräftigen Reaktionen wird der Landesbeauftragte im nächsten Berichtszeitraum überprüfen, ob sich die Auskunfteien auch daran halten.

Bundesweite Beachtung fand ein Urteil des BGH vom 28. Januar 2014 (NJW 2014, 1235), welches insbesondere für Kreditnehmer auch in Sachsen-Anhalt von Bedeutung ist. Zu entscheiden war über einen Auskunftsanspruch der Betroffenen gegenüber einer Auskunftei. Der BGH stellte einerseits klar, dass die Auskunftei die in die Scorewertberechnung einfließenden personenbezogenen, insbesondere die kreditrelevanten Daten, gemäß § 34 Abs. 4 Satz 1 Nr. 4 BDSG preisgeben muss. Nach dieser Vorschrift ist auf Verlangen eine Auskunft zu erteilen über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte und zwar einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form. Andererseits hat nach Ansicht des BGH der Auskunftsanspruch aber auch Grenzen. Die sogenannte Scoreformel, d. h. die abstrakte Methode, mit der ein konkreter Scorewert für eine einzelne Person errechnet wird, muss nicht mitgeteilt werden, da sie ein Geschäftsgeheimnis sei. Dies ist insoweit misslich, als insbesondere Kreditnehmer keine Möglichkeit haben zu erfahren, wie die Einzelwerte, die in die Berechnung eingeflossen sind, gewichtet wurden. Damit können sie nicht nachvollziehen, wie ihre Bonität berechnet wurde.

Nach Ansicht des Landesbeauftragten ist der Bundesgesetzgeber gefordert, die Auskunft über das Scoringverfahren datenschutzfreundlicher zu gestalten. Interessant ist in diesem Zusammenhang ein Gesetzentwurf der Bundestagsfraktion der Grünen (BT-Drs. 18/4864). Dieser Entwurf sieht insbesondere eine Ausweitung des

Auskunftsanspruchs auf die Gewichtung der verwendeten Einzeldaten und die Vergleichsgruppen vor. Die Auskunft soll unverlangt erfolgen. Zudem sollen die Aufsichtsbehörden verpflichtet werden, bei den Auskunfteien die Einhaltung dieser Vorgaben jährlich zu kontrollieren.

14.11 Werbung

Weiterhin Defizite sieht der Landesbeauftragte im Umgang der Wirtschaft mit Kundendaten (vgl. XI. Tätigkeitsbericht, Nrn. 13.2.4; 13.2.5; 13.4.1; 13.4.2). Zwar erkennt er an, dass Werbung ein unverzichtbarer Bestandteil sein mag, um den wirtschaftlichen Erfolg eines Unternehmens sicherzustellen. Der rechtliche Rahmen muss trotzdem gewahrt bleiben.

Deshalb wendet er sich auch gegen Versuche einzelner nicht-öffentlicher Stellen, Werbung per E-Mail (Newsletter) zu versenden, ohne dass die erforderliche ausdrückliche Einwilligung des Kunden vorliegt. Stattdessen werden – in den Allgemeinen Geschäftsbedingungen (AGB) versteckt – vorformulierte Erklärungen für Einwilligungen und „Datenschutzhinweise“ verwendet. Dies reicht jedoch nicht aus, weil Einwilligungen, sofern sie mit anderen Erklärungen schriftlich erteilt werden sollen, besonders hervorzuheben sind. Deshalb wird der Landesbeauftragte im nächsten Berichtszeitraum die AGB von überregional tätigen Unternehmen mit Internetauftritt stichprobenartig überprüfen.

Ebenso wenig hat er Verständnis, wenn auf den gesetzlichen Anspruch des Betroffenen auf Auskunft über die zu seiner Person gespeicherten Daten und deren Herkunft dergestalt reagiert wird, dass nicht wenigstens konkret benannt wird, welche personenbezogenen Daten tatsächlich gespeichert worden sind, sondern nur die Kategorien („Name, Vorname, Adresse“ usw.) angegeben werden.

Solche „Auskünfte“ laufen dem Zweck zuwider, dass der Kunde die über ihn gespeicherten Daten konkret überprüfen und unrichtige Daten (wie etwa auch falsche Schreibweisen) berichtigen lassen kann. Auch verspätete Auskünfte – z. B. erst nach etlichen Monaten und mehreren Erinnerungen der Aufsichtsbehörde – erfüllen nicht die Vorgaben des Bundesdatenschutzgesetzes.

14.12 Aufzeichnung von Telefongesprächen

Mehrfach hatte der Landesbeauftragte Beschwerden bzw. Anfragen zu der Zulässigkeit von Aufzeichnungen von Telefongesprächen zu bearbeiten.

Ein Petent beschwerte sich darüber, dass in einer Taxizentrale sämtliche Telefonate ohne das Wissen der Anrufer aufgezeichnet werden. Selbst einige der beschäftigten Taxifahrer wüssten nicht, dass ihre Anrufe in der Zentrale aufgezeichnet würden. Als Grund für die Aufzeichnung wurde angegeben, dass bei ca. 30.000 monatlich eingehenden Anrufen es häufig zu Fehlern kommt, die mithilfe der Aufzeichnung korrigiert werden könnten. Weiterhin sollte sie insbesondere bei Vorbestellungen zur Beweisführung bezüglich haftungsrechtlicher Ansprüche dienen.

Datenschutzrechtlich sind Aufzeichnungen von Gesprächen im höchsten Maße problematisch, denn das Recht am gesprochenen Wort ist als Teil des allgemeinen Per-

sönlichkeitsrechts durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützt. Dazu gehört auch die Befugnis, selbst zu bestimmen, ob der Kommunikationsinhalt einzig dem Gesprächspartner, einem bestimmten Personenkreis oder der Öffentlichkeit zugänglich sein soll. Das Recht am gesprochenen Wort erstreckt sich damit auf die Auswahl der Personen, die Kenntnis vom Gesprächsinhalt haben sollen. Es ist nicht identisch mit dem Schutz der Privatsphäre. Deshalb kommt es nicht darauf an, ob ein Gespräch einen vertraulichen Inhalt hat (BVerfG, NJW 2002, 3619).

Gesprächsaufzeichnungen stellen eine Speicherung personenbezogener Daten dar, denn sie geben Auskunft darüber, wer mit wem und worüber gesprochen hat. Betroffene Personen sind der Anrufer, der Angerufene oder Dritte, sofern der Gesprächsinhalt etwas über sie aussagt. Gesprächsaufzeichnungen sind daher nur zulässig aufgrund einer Rechtsvorschrift, die dies erlaubt oder anordnet oder einer freiwilligen und informierten Einwilligung gemäß § 4a BDSG.

Eine Einwilligung kam in diesem Fall schon deshalb nicht in Betracht, weil den anrufenden Kunden und auch einigen beschäftigten Taxifahrern die Gesprächsaufzeichnung nicht bekannt war.

Aber auch Rechtsvorschriften gestatteten diese im hier vorliegenden Fall nicht:

§ 28 Abs. 1 Nr. 1 BDSG hätte für die Gesprächsaufzeichnung verlangt, dass sie für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses mit dem Betroffenen erforderlich ist. Dies ist hier nicht der Fall. Für die Entgegennahme des Anrufes reichen bei unklaren Bestellungen Nachfragen durch den Angerufenen. Dabei wird geschultes Personal in der Lage sein festzustellen, welcher Anrufer an welchem Ort abgeholt und zu welchem Ort gebracht werden möchte. Nicht zu berücksichtigen ist hier der Zweck der Beweissicherung für haftungsrechtliche Ansprüche des Taxiunternehmens. § 28 Abs. 1 Nr. 1 BDSG setzt einen unmittelbaren sachlichen Zusammenhang zwischen der beabsichtigten Verwendung und dem konkreten Zweck des Schuldverhältnisses voraus (Simitis, in: Simitis, BDSG, § 28 Rn. 57). Dies liegt bei der Beweissicherung für haftungsrechtliche Ansprüche nicht mehr vor.

Auch § 28 Abs. 1 Nr. 2 BDSG scheidet als Rechtsgrundlage aus. Danach wäre die Gesprächsaufzeichnung zulässig, wenn sie zur Wahrung berechtigter Interessen der Taxizentrale erforderlich gewesen wäre und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen überwiegt. Als berechtigtes Interesse käme hier u. U. auch die Beweissicherung im o. g. Sinne in Betracht, die aber in aller Regel – wie bereits dargelegt – keine Gesprächsaufzeichnung erfordert. Im Übrigen würden auch die berechtigten Interessen der Anrufer überwiegen. Allein das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, reicht nicht aus, um die Verletzung des Rechts am gesprochenen Wort zu rechtfertigen (vgl. BGH, NJW 2003, 1727).

In einem weiteren Fall wurde der Landesbeauftragte befragt, ob eine Gesprächsaufzeichnung bei Anwahl einer sogenannten „Störfall-Nummer“ eines Versorgungsunternehmens (hier: Stadtwerke) zulässig ist. Dabei sollte auf der Homepage des Unternehmens und in der Kundenzeitung auf den Umstand, dass eine Aufzeichnung erfolgt, hingewiesen werden. Die Aufzeichnung sollte ohne vorherige Ansage beginnen und drei Monate gespeichert werden. Als Grund für die Aufzeichnung wurden die

Abwehr von Schadensersatzansprüchen sowie die Erhöhung der Qualität der Störfallbeseitigung angegeben.

Auch hier kann nicht davon ausgegangen werden, dass alle Anrufer in die Gesprächsaufzeichnung gemäß § 4a BDSG eingewilligt haben. Zwar ist eine schlüssig erklärte Einwilligung dann möglich, wenn dem Anrufer die Aufzeichnung bekannt ist. Dies wird jedoch nicht immer der Fall sein, da nicht anzunehmen ist, dass jeder Anrufer bei einem Störfall die Homepage oder die Kundenzeitung derart sorgfältig liest, dass er von der Aufzeichnung Kenntnis erlangt und erst dann zum Hörer greift. Die vollständige Kenntnis über den Zweck der Aufzeichnung und die beabsichtigte Verwendung ist aber Voraussetzung dafür, dass überhaupt eingewilligt werden kann (Simitis a. a. O., § 4a Rn. 72).

Ebenso wenig liegen hier die Voraussetzungen einer Erlaubnisvorschrift vor. § 28 Abs. 1 Nr. 1 BDSG scheidet aus, da die Aufzeichnung nicht für die Durchführung eines Versorgungsvertrages erforderlich ist. Auch hier genügt geschultes Personal, um die Störungsmeldung entgegenzunehmen und Abhilfemaßnahmen einzuleiten.

Bei der Interessensabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG ist wiederum zu berücksichtigen, dass allein das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, nicht ausreicht, um die Verletzung des Rechts am gesprochenen Wort zu rechtfertigen. Rechtlich möglich wäre eine Gesprächsaufzeichnung nach dieser Vorschrift bestenfalls in Notwehrsituationen oder notwehrähnlichen Lagen (vgl. BGH, NJW 2003, 1727). Diese könnten u. U. gegeben sein, wenn sich im Verlauf des Anrufs Anzeichen für akute Gefahrenlagen ergeben, z. B. Bedrohungen für Leib und Leben oder erhebliche Gefährdungen für Sachwerte. Inwiefern mit derartigen Anrufen bei der „Störfall-Nummer“ zu rechnen ist, wurde aber von den Stadtwerken nicht vorgetragen.

Der Landesbeauftragte empfiehlt daher in vergleichbaren Situationen dringend, vor einer Gesprächsaufzeichnung die Einwilligung des Anrufers einzuholen. Dazu könnte eine Bandansage vor dem Gespräch auf Zweck und die vorgesehenen Verarbeitungen hinweisen.

Wird die Einwilligung zur Aufzeichnung durch den Anrufer erteilt, ist darauf zu achten, dass nur eine Verarbeitung und Nutzung zu dem den Anrufern bekannten Zweck erfolgt. Lässt dieser Zweck keine Auswertung des Verhaltens der Beschäftigten des Versorgungsunternehmens zu, so hat sie zu unterbleiben.

Sofern der Anrufer keine Aufzeichnung wünscht, muss sie abgestellt, sein Begehren aber gleichwohl entgegengenommen werden. Sollten während des Gesprächs Anzeichen für Notwehrsituationen oder notwehrähnliche Lagen entstehen, könnte der Angerufene im Einzelfall eine Aufzeichnung auch ohne Einwilligung aktivieren.

Da bei den hier bewerteten Gesprächsaufzeichnungen regelmäßig auch Äußerungen der Beschäftigten der verantwortlichen Stellen aufgenommen werden, ist auch diesbezüglich zu prüfen, ob deren wirksame Einwilligung oder die Voraussetzungen einer Erlaubnisvorschrift vorliegen. Auch für den Fall, dass eine Einwilligung der Beschäftigten nicht erforderlich ist, weil sich die verantwortliche Stelle gegenüber ihnen z. B. auf § 32 BDSG beruft, ist regelmäßig eine Information an sie über die Aufzeichnung erforderlich.

Die Aufzeichnung von Telefongesprächen ist nicht nur datenschutzrechtlich relevant, sondern kann in Falle eines Strafantrags auch strafrechtlich verfolgt werden. Nach § 201 Abs. 1 Nr. 1 StGB wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt. Eine Einwilligung des Betroffenen lässt den Tatbestand entfallen oder wirkt zumindest rechtfertigend (vgl. Lenckner/Eisele, in: Schönke/Schröder, Strafgesetzbuch, § 201 Rn. 13).

14.13 Wohnungswirtschaft

Auch bei großen Wohnungsunternehmen bestehen oft Unsicherheiten, welche Auskünfte von Mietinteressenten datenschutzrechtlich zulässig eingeholt werden dürfen. Aus diesem Grunde hat der Düsseldorfer Kreis als Zusammenschluss der Aufsichtsbehörden im nicht-öffentlichen Bereich eine „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten“ herausgegeben (**Anlage 36**).

Darin wird insbesondere darauf hingewiesen, dass nur solche Fragen gestellt werden dürfen, deren Beantwortung zur Durchführung des Mietvertrages erforderlich ist oder an deren Beantwortung ein berechtigtes Interesse besteht. Entscheidend für die Erhebung und Speicherung einzelner personenbezogener Daten ist insbesondere, ob lediglich ein Besichtigungstermin vereinbart wurde, der Mietinteressent bereits erklärt hat, eine Wohnung mieten zu wollen oder der Vermieter sich bereits für einen bestimmten Interessenten entschieden hat.

Der Landesbeauftragte hat die Orientierungshilfe bei Wohnungsunternehmen bekannt gemacht und geht davon aus, dass die darin enthaltenen Regelungen beachtet werden. Dies wird er im nächsten Berichtszeitraum stichprobenartig überprüfen.

15 Videoüberwachung

15.1 Videoüberwachung durch öffentliche Stellen

15.1.1 Objektsicherung

Bereits in früheren Berichten wurden Erläuterungen zur Videoüberwachung gegeben (z. B. IX. Tätigkeitsbericht Nr. 19.4). Nun fragte eine öffentliche Stelle den Landesbeauftragten im Rahmen der Überprüfung der Gebäudesicherheit zur Ausgestaltung der Videoüberwachung an. Eine Vielzahl von Kameras wurde bereits betrieben (u. a. Toreinfahrt von hinten, Kamera im Eingangsbereich, Dachkamera).

Hierzu wies der Landesbeauftragte zunächst darauf hin, dass für jede Videoüberwachungsmaßnahme gesondert zu überprüfen ist, ob und in welchem Umfang eine Beobachtung und Aufzeichnung stattfinden kann. Dabei ist aus datenschutzrechtlicher Sicht insbesondere zu berücksichtigen, welche Personen gelegentlich oder regelmäßig vom Überwachungsbereich erfasst werden. Weiter wurde dargelegt, dass zwischen der reinen Beobachtung durch optisch-elektronische Einrichtungen im Sinne einer Datenerhebung und einer (Video-)Aufzeichnung und Aufbewahrung für mehrere Tage als datenschutzrechtliche Speicherung zu unterscheiden ist. Infolge der erheblich weitergehenden Betroffenheit durch Aufzeichnung ist im jeweiligen Einzelfall ein demgemäß erheblich höherer Begründungsaufwand erforderlich.

Die Videoüberwachung ist grundrechtsrelevant. Soweit natürliche Personen erfasst werden, stellt dies zunächst einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung (vgl. BVerfGE 65, 1, 45; BVerfG 1 BvR 2368/06, DVBl 2007, 497). Die offene Videoüberwachung kann und soll abschreckend wirken und insofern das Verhalten der Betroffenen lenken. Durch die Aufzeichnung des gewonnenen Bildmaterials werden zusätzlich die beobachteten Lebensvorgänge technisch fixiert und können in der Folge abgerufen, aufbereitet und ausgewertet sowie mit anderen Daten verknüpft werden. Der Grundrechtseingriff wird somit erheblich verstärkt (vgl. dazu BVerfG, a. a. O.). Der Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung bedarf daher stets einer besonderen Rechtfertigung.

Die Unterscheidung zwischen der Aufnahme von öffentlich zugänglichen und nicht öffentlich zugänglichen Räumen ist von Bedeutung. Hintergrund ist die Tatsache, dass Liegenschaften und Behördengebäude des Landes nicht notwendig dazu bestimmt sind, von einem unbestimmten Personenkreis betreten und genutzt zu werden. Soweit dies der Fall ist, handelt es sich nicht um öffentlich zugängliche Räume. Dem stehen Bereiche gegenüber, die für den öffentlichen Verkehr gewidmet worden sind oder dazu dienen, von jedermann genutzt oder betreten zu werden. Dies sind z. B. Schalterhallen, Ausstellungsräume, Eingangsbereiche öffentlicher Gebäude oder auch Gehwege vor dem Gebäude im öffentlichen Straßenraum oder Häuserfassaden. Für den Umfang der Zulässigkeit von Aufzeichnungen sind z. B. Aspekte des Aufzeichnungsbereiches, der Schärfe und der Schärfentiefe sowie insbesondere der Dauer der Aufzeichnung (24 Stunden am Tag; anlassbezogen z. B. auf Klingeldruck) von Bedeutung.

Datenschutzrelevant sind die Vorgänge der Videoüberwachung jedoch nur, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Der Personenbezug ist jedoch beim Einsatz von Videoüberwachungstechnik regelmäßig anzunehmen. Die Erfassung von Personen ist gerade Ziel der Videoüberwachung. Ausnahmen bestehen allenfalls dann, wenn infolge der äußerst geringen Pixelzahl und des Ziels der Kameraverwendung nicht von dem Erfassen personenbezogener oder personenbeziehbarer Informationen auszugehen ist. Anders ist die Lage auch bei Attrappen. Dort werden keine personenbezogenen Daten erhoben, verarbeitet oder genutzt, sodass auch keine Rechtsgrundlage nötig wäre. Allerdings wird ein Überwachungsdruck erzeugt. Mit dem Dritten Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 21. Juli 2015 (GVBl. LSA S. 365) wurde dazu in § 30 DSG LSA ergänzend vorgesehen, dass die Verwendung von Attrappen nur unter Voraussetzungen zulässig ist wie bei funktionsfähigen Geräten.

Als Rechtsgrundlage für eine optisch-elektronische Beobachtung öffentlich zugänglicher Bereiche kommt die Regelung des § 30 DSG LSA selbst in Betracht. Danach dürfen öffentliche Stellen Beobachtungen vornehmen zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen. Auf dieser Grundlage sind daher Maßnahmen zur Objektsicherung von Gebäuden grundsätzlich möglich. Das Hausrecht gibt die Befugnis, darüber zu entscheiden, wer abgeschlossene Räume oder befriedetes Besitztum betreten darf. Gegebenenfalls wäre es bei entsprechender Begründung auch möglich, Videotechnik in unübersichtlichen Bereichen einzusetzen, um Dritte vor dem Risiko zu schützen, ei-

ner Straftat ausgesetzt zu sein. Auch der Schutz vor Sachbeschädigungen oder Diebstahl fällt in den Bereich, wie die Absicht der Abschottung sensibler Bereiche innerhalb eines Verwaltungsgebäudes. Da der Einsatz von Videoüberwachungstechnik überwiegend präventiven Zwecken (Gefahrenabwehr) dient, ist zu berücksichtigen, dass die bloße Behauptung oder Vermutung einer Gefährdungslage für die Zulässigkeit nicht ausreichend ist. Auch wenn nicht das Vorliegen konkreter Vorfälle der Vergangenheit zu fordern ist, müssen jedoch konkrete Anhaltspunkte bestehen, die das Bestehen einer Gefährdungslage nach der allgemeinen Lebenserfahrung wahrscheinlich erscheinen lässt. Bei der Gefahrenprognose sind die Aspekte der Höhe möglicher Schäden und insbesondere der Wahrscheinlichkeit eines Schadenseintritts zu berücksichtigen.

Weitere Voraussetzung nach § 30 DSG LSA ist, dass jeweils im Einzelfall der Einsatz von Videoüberwachungstechnik auch im Hinblick auf Art und Umfang erforderlich, d. h. im Sinne der Rechtsprechung des Bundesverfassungsgerichtes unerlässlich ist. Demnach ist für jede Maßnahme zu überprüfen, ob eine permanente Überwachung erfolgen muss bzw. ob sie zeitlich begrenzt werden kann (z. B. außerhalb der Dienstzeiten, anlassbezogene Aktivierung). Es wäre zu fragen, ob es einer Aufzeichnung bedarf oder ob eine Übertragung auf einen Monitor ausreicht (z. B. Öffnung des Tores auf Anforderung durch den Pfortendienst). Insoweit wäre zuvor zudem auszuschließen, dass andere Zugangskontrollsysteme als mildere Mittel in Betracht kommen. Im Hinblick auf den Überwachungsbereich stellt sich die Frage, ob dieser räumlich beschränkt werden kann (digitales Ausblenden nicht überwachungsbedürftiger Zonen).

Von besonderer Bedeutung ist der Aspekt der auch verfassungsrechtlich vorgegebenen Verhältnismäßigkeit. Nach § 30 DSG LSA sind entsprechende Maßnahmen lediglich dann zulässig, wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Personen, die sich im Aufnahmebereich der Einrichtung befinden, überwiegen. Demgemäß ist für jede beabsichtigte Maßnahme zu prüfen, welche Personen sich im Aufnahmebereich aufhalten könnten. Im Rahmen der Interessenabwägung ist u. a. die Art der Beeinträchtigung maßgebend für die Beurteilung der Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung. Dabei kann z. B. eine Rolle spielen, ob analoge Aufzeichnungen stattfinden oder digitale, die ggf. auch biometrischen und anderen Datenabgleichen zugänglich sind. Maßgeblich ist auch, ob die betroffenen Personen einen Anlass gegeben haben, wie dieser beschaffen ist und wie zahlreich (Streubreite) sie in den Wirkungsbereich der Maßnahmen einbezogen werden (vgl. BVerfG, a. a. O.). Weitere Aspekte der Interessenabwägung sind die permanente und lückenlose Überwachung bzw. die Erfassung von Bereichen, die der ungezwungenen und freien Entfaltung der Persönlichkeit dienen (Kantinen, Raucherecke, Wartebereiche). Um entsprechend der gesetzlichen Vorgabe die Abwägung mit den Interessen der von der Aufzeichnung möglicherweise Betroffenen vornehmen zu können, ist eine differenzierte Beschreibung des Beobachtungszweckes geboten, mit dem die eventuell überwiegenden Persönlichkeitsinteressen abzuwägen sind. Damit ist im Hinblick auf die weitere Verwendung der ggf. gespeicherten Informationen eine Zweckbindung festgelegt.

Den der Anfrage beigefügten Bildschirmausdrucken war zu entnehmen, dass zwei Kameras den Bereich des öffentlichen Fußweges komplett sowie der Straße und des gegenüberliegenden Straßenrandes über eine Länge aufzeichnen, die (unter Berücksichtigung des abgebildeten PKWs geschätzt) ca. 30 m betrug. Hiergegen be-

standen erhebliche inhaltliche Bedenken. Ein Zusammenhang mit den im § 30 DSG LSA benannten Rechtfertigungsgründen (Hausrecht, Eigentumsschutz, Zugangsberechtigung) war hier nicht mehr erkennbar. Die Wahrung der allgemeinen Sicherheit auf der Straße wird von § 30 DSG LSA nicht abgedeckt. Dem Aspekt der Zugangskontrolle kann anderweitig und mit milderen Mitteln Rechnung getragen werden. Ob der Aspekt des Objektschutzes im Sinne der Bewahrung einer Häuserfassade vor Beschädigungen in Betracht kommt, wäre zu prüfen gewesen. Zumindest dürfte aber eine Erfassung eines Bereiches, der über 1 m von der Gebäudefassade entfernt ist, mit den Persönlichkeitsinteressen der sich im Straßenraum befindlichen Passanten nicht mehr zu vereinbaren sein. Hierzu verwies der Landesbeauftragte auf eine Entscheidung des Amtsgerichts Berlin-Mitte (18. Dezember 2003, Az. 16 C 427/02, juris) zu § 6b BDSG.

Ergänzend wurde auf folgende Aspekte aufmerksam gemacht: Es ist notwendig, die Möglichkeit der Beobachtung für die Betroffenen, die sich im Aufnahmebereich befinden können, erkennbar zu machen (§ 30 Abs. 2 DSG LSA). Der Beobachtungsvorgang muss wahrnehmbar sein, die Einrichtung muss deutlich sichtbar sein und auf die Beobachtung muss deutlich durch Schilder hingewiesen werden. Weiterhin ist das Gebot unverzüglicher Löschung nach § 30 Abs. 4 DSG LSA zu beachten, wenn die Daten zur Zweckerreichung nicht mehr erforderlich sind oder in Ausnahmefällen die Schutzwürdigkeit von Interessen Betroffener eine Löschung gebietet. Schließlich wurde angeregt, die Erforderlichkeit regelmäßig zu überprüfen. Auch auf die Notwendigkeit technischer und organisatorischer Mindestanforderungen an eine sichere Datenverarbeitung wurde hingewiesen (§ 6 Abs. 2 DSG LSA). Insbesondere ist dem Schutz vor dem Zugriff Unbefugter auf die Überwachungsbilder Rechnung zu tragen. Auf weitere Informationen in technischer und organisatorischer Hinsicht (Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik in Zusammenarbeit mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über Schutzprofile für Videoüberwachungsanlagen (siehe Homepage des Landesbeauftragten; vgl. auch VIII. Tätigkeitsbericht, Nr. 12.4)) wurde ergänzend hingewiesen. Zusätzlich war die Verfahrensvorgabe zu berücksichtigen, dass verantwortliche Stellen automatisierte Verfahren, mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, in einem Verfahrensverzeichnis nach § 14 Abs. 3 DSG LSA festzulegen haben.

§ 30 DSG LSA regelt nicht die Zulässigkeit von Beobachtungen mittels optisch-elektronischer Einrichtungen von solchen Bereichen, die nicht öffentlich zugänglich sind. Auch insoweit ist jedoch zu berücksichtigen, dass Datenerhebungen und Speicherungen in Bezug auf natürliche Personen grundrechtsrelevant sind und demgemäß nur insoweit in Betracht kommen können, als dies zur Erfüllung der Aufgabe der öffentlichen Stelle erforderlich ist (§§ 9 Abs. 1, 10 Abs. 1 DSG LSA). Bei der Prüfung der Frage, ob Art und Ausmaß des Grundrechtseingriffs unter Berücksichtigung der Interessen der Dienststelle erforderlich und verhältnismäßig sind, sind die spezifischen Schutzinteressen der Besucher und insbesondere der Beschäftigten der Dienststelle zu berücksichtigen. Im Hinblick auf die Erfassung von Mitarbeitern öffentlicher Stellen in nicht öffentlich zugänglichen Bereichen durch Videoüberwachungen müssen die von der Rechtsprechung hierzu aufgestellten engen Anforderungen erfüllt sein. Auch wenn es derzeit keine spezifischen gesetzlichen Ausgestaltungen gibt, ist danach Folgendes zu berücksichtigen:

Die Videoüberwachung eines Beschäftigten ist eine Maßnahme mit hoher Eingriffsintensität. Sie bewirkt einen hohen psychischen Anpassungsdruck, der die Freiheit, selbstbestimmt zu handeln, einschränkt. Es besteht die Unsicherheit, ob Verhaltensweisen notiert, gespeichert und weitergegeben werden mit der Folge, dass Beschäftigte nicht auffallen wollen. Zudem sind die betroffenen Beschäftigten in der Regel nicht Ursachengeber (Beobachtung Unschuldiger). Sie befinden sich zumeist auch nicht nur kurzfristig in dem Beobachtungsbereich und verweilen dort auch nicht freiwillig, sondern aufgrund der Zuweisung durch den Dienstherrn. In der Folge dieser erheblichen Eingriffsintensität ist eine Videoüberwachung in der Regel nur zulässig, wenn eine notwehrähnliche Lage gegeben ist (Bundesarbeitsgericht, Urteil vom 27. März 2003, Az. 2 AZR 51/02, juris; vgl. auch XI. Tätigkeitsbericht, Nr. 4.17.3).

Soweit keine heimliche oder dauerhafte Beobachtung von Beschäftigten vorgesehen ist, sondern lediglich die Überwachung von Eingangsbereichen, Bürofluren, Parkplätzen oder Sicherheitsbereichen, ist auch dort die nicht unerhebliche Intensität der Überwachung zu berücksichtigen, auch wenn die Erfassung lediglich Nebenfolge der Wahrung von Sicherheitsinteressen ist. Diese Sicherheitsinteressen vermögen das Schutzinteresse des Beschäftigten an der Vermeidung ständigen Überwachungsdrucks zu überwiegen, wenn durch entsprechende Maßnahmen Ausgleiche geschaffen sind. Werden die Beschäftigten nur gelegentlich bei Durchquerung bestimmter Bereiche erfasst, sind diese Bereiche den Beschäftigten erkennbar und bestehen hinreichende Rückzugsmöglichkeiten und werden sensible Bereiche (sanitäre Räumlichkeiten, Pausen- und Aufenthaltsräume) ausgenommen, können die Überwachungen vertretbar sein. Insoweit ist die Zweckbindung besonders zu berücksichtigen, da die vorhandenen Informationen keinesfalls zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz der Beschäftigten verwendet werden dürfen. § 69 Nr. 2 PersVG LSA wäre zu beachten.

15.1.2 Wildmonitoring durch Jagdbehörden

Mit dem Dritten Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 21. Juli 2015 (GVBl. LSA S. 365) wurde für die Nutzung von Wildkameras durch öffentliche Stellen in § 48b Landesjagdgesetz eine differenzierte Regelung aufgenommen, die auch auf intensive Beratungen durch den Landesbeauftragten zurückgeht (siehe auch Nr. 3.1.3). Danach können Jagdbehörden für Einzelbildaufnahmen optisch-elektronische Einrichtungen verwenden zum Schutz besonders geschützter Tierarten oder für wissenschaftliche Untersuchungen zu deren Wiederbesiedlung; die Behörden können sich Dritter bedienen. Es dürfen aber keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von Personen, die sich im Aufnahmebereich befinden, überwiegen. Zu Wildkameras im nicht-öffentlichen Bereich siehe Nr. 15.2.13.

15.2 Videoüberwachung durch nicht-öffentliche Stellen

15.2.1 Allgemeines

Auch durch nicht-öffentliche Stellen wird Videoüberwachung häufig zum Zweck der Gefahrenabwehr oder zur Ermittlung von Schädigern eingesetzt. Diese Überwachung geschieht seit geraumer Zeit geradezu inflationär: beim Einkauf, in Restaurants, Parkhäusern, Bussen, Bahnen und Taxis, am Arbeitsplatz und sogar im Wald.

Videoüberwachung erfolgt durch Handelsketten, Einzelhändler, Arbeitgeber und private Haushalte. Videoüberwachung wird betrieben aus PKW, Fassaden, Fenstern, Decken, versteckt aus Regalen und mittlerweile sogar aus der Luft (derzeit sollen sich in Deutschland 300.000 Drohnen, die zum Tragen von Kameras geeignet sind, allein im privaten Besitz befinden (Gola, Bundesdatenschutzgesetz, 12. Auflage 2015, § 6b Rn. 7b)).

Sobald mithilfe einer Videokamera bestimmbare Personen abgelichtet bzw. gespeichert werden, also personenbezogene Daten erhoben und verarbeitet werden, sind die Voraussetzungen des Bundesdatenschutzgesetzes einzuhalten, sofern die Tätigkeit nicht als persönlich oder familiär einzuordnen ist (siehe Nr. 15.2.2). Die Identifizierung einer Person ist im Falle einer Videoaufnahme nicht nur anhand ihres Gesichtes möglich, sondern auch durch Abbildung von Körperhaltung, Kleidung, mitgeführten Gegenständen oder sonstigen Umständen. Selbst die bloße Aufnahme einer Sache – z. B. eines Kraftfahrzeugs – zu einer bestimmten Zeit an einem bestimmten Ort kann Informationen über natürliche Personen offenbaren (vgl. Verwaltungsgericht Schwerin, Beschluss vom 18. Juni 2015, Az. 6 B 1637/15 SN, juris).

Die Videoüberwachung in öffentlich zugänglichen Räumen regelt § 6b BDSG, bei der Videoüberwachung von Beschäftigten ist § 32 Abs. 1 BDSG zu berücksichtigen, bei nicht öffentlich zugänglichen Räumen § 28 Abs. 1 Nr. 2 BDSG. Grundsätzlich ist Videoüberwachung nur dann zulässig, wenn die verantwortliche Stelle dafür ein berechtigtes Interesse hat, welches sie auch nachweisen kann. Zudem dürfen regelmäßig keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen derjenigen, die sich im Erfassungsbereich einer Videokamera befinden, überwiegen. Die wesentlichen Voraussetzungen der Videoüberwachung hat der Düsseldorfer Kreis in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“[11] zusammengefasst. Aktuell wurde diese Orientierungshilfe ergänzt durch einen Zusatz zur Videoüberwachung in Schwimmbädern.

Darüber hinaus ist bei der Videoüberwachung das Recht am eigenen Bild zu berücksichtigen. Danach dürfen Bildnisse grundsätzlich nur mit Einwilligung der abgelichteten Person verbreitet oder öffentlich zur Schau gestellt werden, § 22 KunstUrhG. Ohne Einwilligung ist dies in den Fällen des § 23 KunstUrhG möglich, z. B. bei Bildern, auf denen eine Person nur als Beiwerk einer Örtlichkeit erscheint. Verstöße gegen das Recht am eigenen Bild können auf Antrag als Straftat gemäß § 33 KunstUrhG verfolgt werden. Im Zivilrechtsweg können Schadensersatz, Vernichtung der Ablichtungen und die Unterlassung weiterer Aufnahmen verlangt werden.

Bei der Prüfung zahlreicher Eingaben musste der Landesbeauftragte feststellen, dass die gesetzlichen Vorgaben oft keine Berücksichtigung fanden. Vielfach wurden Kunden, Beschäftigte oder auch Passanten unangemessen überwacht. So wurden auf Betreiben des Landesbeauftragten viele Kameras deaktiviert, Speicherfristen teilweise erheblich gekürzt, Erfassungsbereiche korrigiert oder in erforderlichem Umfang Hinweisschilder angebracht.

[11] http://lsaurl.de/VideoOH

Vorsicht ist geboten, wenn Sicherheitsfirmen oder Hersteller mit extensiver Videoüberwachung offensiv werben. Beide informieren häufig lediglich über die technischen Möglichkeiten, nicht aber über die rechtlichen Voraussetzungen. Letztere sind aber durch die verantwortlichen Stellen, d. h. die Stellen, die für sich selbst mithilfe der Videoüberwachung personenbezogene Daten erheben, verarbeiten oder nutzen, einzuhalten. Für eine datenschutzrechtliche Beratung vor der Anschaffung der Videoanlage steht der Landesbeauftragte zur Verfügung. Diese kann vor Fehlinvestitionen bewahren.

15.2.2 Videoüberwachung durch Privatpersonen

Häufig muss der Landesbeauftragte Privatpersonen darauf hinweisen, dass auch deren Videoüberwachung den Regelungen des BDSG und damit Beschränkungen unterliegt (allgemeine Hinweise zur Rechtslage, vgl. XI. Tätigkeitsbericht, Nr. 4.17.2).

Zwar ist das BDSG gemäß § 1 Abs. 2 Nr. 3 ausnahmsweise nicht anwendbar, soweit die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten „ausschließlich für persönliche oder familiäre Tätigkeiten“ erfolgt. Zu der Frage, wann dieses Merkmal erfüllt ist, hat der EuGH am 11. Dezember 2014 ein bedeutendes Urteil gefällt (ZD 2015, 77). Zu entscheiden war, ob eine Videoüberwachung an einem Einfamilienhaus zum Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens ausschließlich zu persönlichen oder familiären Tätigkeiten vorgenommen wird, wenn zumindest auch der öffentlich zugängliche Bereich erfasst wird.

Der EuGH hat zunächst festgestellt, dass angesichts der Bedeutung des Rechts auf Achtung des Privatlebens der Begriff der „persönlichen oder familiären Tätigkeiten“ eng auszulegen ist. Erstreckt sich eine Videoüberwachung wie in diesem Fall auch nur teilweise auf den öffentlichen Raum, so kann sie nicht als ausschließlich persönliche oder familiäre Tätigkeit angesehen werden. Die Folge ist, dass hier das BDSG anzuwenden und eine Videoüberwachung nur zulässig ist, wenn die Voraussetzungen des § 6b erfüllt sind. Der Landesbeauftragte begrüßt dieses Urteil und hat Privatpersonen stets auf diese Vorschrift verwiesen.

Beispielhaft seien hier zwei typische Fallgestaltungen dargestellt: In einem zu prüfenden Fall beobachtete ein Grundstücksbesitzer Teile seines schwer einsehbaren Grundstücks mit Videotechnik. Eine Aufzeichnung fand nicht statt. Die Videoüberwachung diene nach Angaben des Betreibers ausschließlich der Einsichtnahme des eigenen Grund und Bodens, obwohl die Videokamera Teile des Gehweges und der Straße vor dem Haus und Teile des Nachbargrundstücks miterfasste. Der Betreiber wurde vom Landesbeauftragten schriftlich darauf hingewiesen, dass eine grundlose Überwachung öffentlich zugänglicher Bereiche unzulässig sei. Weiterhin wurde ihm nahegelegt, die Videokamera so auszurichten, dass ausschließlich nicht öffentlich zugängliche Bereiche seines eigenen Grundstücks beobachtet werden. Dem kam er schließlich nach.

In einem anderen Fall wurde durch eine Privatperson eine Videoüberwachung des öffentlich zugänglichen Raumes, nämlich Haustür und Briefkasten, Garagentore, Hausfront, Gehweg und Teile der befahrbaren Straße vor dem Haus sowie des Nachbargrundstücks durchgeführt. Die Videoüberwachung erfolgte nach Angaben des Betreibers zur Abwendung von Sachbeschädigungen. Die wiederholten Sachbeschädigungen an Kraftfahrzeug und Briefkasten des Betreibers wurden durch Fotos

dokumentiert und bei der örtlichen Polizei zur Anzeige gebracht. In diesem Fall war die Überwachung des öffentlich zugänglichen Bereiches des eigenen Privatgrundstückes und bis zu einem Meter davor gemäß § 6b BDSG zulässig. Eine Verletzung schutzwürdiger Interessen Betroffener war nicht anzunehmen, weil sich Betroffene nur dann einer Beobachtung aussetzen würden, wenn sie sich in unmittelbarer Nähe der Eingangstür oder der Garagentore aufhalten würden. Dass jedoch ebenfalls Teile der Straße und Teile des Nachbargrundstückes mitbeobachtet wurden, war unzulässig. Der Betreiber der Videoanlage wurde auf diesen Umstand hingewiesen und aufgefordert, die Videokameras so auszurichten, dass lediglich die Hausfassade und der Stellplatz für das Fahrzeug erfasst sind.

Da der Landesbeauftragte bei dem Betreiber zunächst auf wenig Verständnis stieß, wurde die Ausrichtung der Videokameras vor Ort überprüft und der Betreiber darauf hingewiesen, dass die Möglichkeit bestehe, ein Zwangsgeld festzusetzen, wenn die Ausrichtung der Kameras nicht entsprechend angepasst werde. Letztlich entschied sich der Betreiber, die problematische Kamera zu demontieren.

Sollten sich Nachbarn von einer privaten Videoüberwachung beeinträchtigt fühlen, können sie – neben dem Landesbeauftragten – zusätzlich auch Zivilgerichte und Schieds- oder Schlichtungsstellen anrufen. Auskünfte erteilen die Gemeinden und Amtsgerichte, die Notar- und die Rechtsanwaltskammer Sachsen-Anhalt.

15.2.3 Videoüberwachung in Einkaufszentren

Bei den Verkaufsräumen von Einzelhändlern (vgl. XI. Tätigkeitsbericht, Nr. 4.17.3) handelt es sich ebenso um öffentlich zugängliche Räume wie bei den Publikumsbereichen von Einkaufszentren, sog. Shoppingmalls, also den Ladenstraßen „zwischen den Läden“. Die Videoüberwachung solcher Kundenbereiche ist nur im Rahmen des § 6b BDSG zulässig, also soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Vergleicht man die Publikumsbereiche im Einzelhandel und in Einkaufszentren aus datenschutzrechtlicher Sicht, stellt man erhebliche Unterschiede fest. Während der Einzelhändler als Besitzer unübersichtlicher Verkaufsräume mit der Videoüberwachung Ladendiebstähle zu verhindern oder aufzudecken versucht, um seine Inventurdifferenzen im Rahmen zu halten, werden die Ziele einer Videoüberwachung in einer Mall andere sein. Das Management der Mall tritt in der Regel nicht als Einzelhändler auf, sondern in erster Linie als Vermieter der einzelnen Ladenlokale. Es ist keineswegs Aufgabe des Centerbetreibers, durch Verhinderung oder Aufklärung von Diebstählen und Sachbeschädigungen bei Dritten deren Eigentum zu schützen sowie Körperverletzungen und Belästigungen gegenüber Kunden zu verhindern. Maßnahmen im Rahmen der Generalprävention und der Aufklärung von Straftaten sind primär öffentliche Aufgaben – auch auf privatem, jedoch öffentlich zugänglichen Grund und Boden. Das schien der Betreiber einer großen Kette von Einkaufszentren, auch mit Objekten in Sachsen-Anhalt, aus dem Blick verloren zu haben.

Zu beachten ist, dass es in den Ladenstraßen in der Regel gastronomische Angebote gibt, die Kunden zu längerem Verweilen, zum Verzehr von Speisen und Getränken und zur Kommunikation mit Dritten einladen (vgl. Nr. 15.2.4). Die Kunden werden aber auch schlicht von einem Laden zum nächsten schlendern, sich die Schaufens-

ter ansehen und hier und da etwas kaufen. Eine Videoüberwachung in solchen Fällen würde die Personen über einen längeren Zeitraum verfolgbar machen. Hierdurch können die schutzwürdigen Interessen der Betroffenen unzulässig beeinträchtigt sein.

Mit einem Centermanagement wurde die Übereinkunft erzielt, dass ausschließlich in den Parkhäusern/Tiefgaragen der Zentren zum Zwecke des Eigenschutzes und der Sicherheit folgende Bereiche mit Videokameras beobachtet werden dürfen:

- Ein- und Ausfahrten, Schrankenanlagen und kritische Kreuzungsbereiche,
- Frauenparkplätze, Notrufsäulen,
- Kassenautomaten.

Sämtliche Kameras in den Ladenstraßen durften nicht weiterbetrieben werden. Die Umsetzung dieser Übereinkunft wurde an drei Standorten des Betreibers in Sachsen-Anhalt überprüft.

Nach Abschluss des Verfahrens war durch den Landesbeauftragten festgestellt worden, dass viele Ladenbetreiber in einem der Center ihre Geschäfte in teils erheblichem Umfang mit Videoüberwachungsanlagen ausgestattet hatten. Mit sämtlichen Mietern dieses Centers hatte der Landesbeauftragte sodann schriftlich Kontakt aufgenommen, um sie auf den datenschutzrechtlich gesetzten Rahmen für eine zulässige Videoüberwachung hinzuweisen. Dazu zählte u. a. eine Speicherfrist von 48 Stunden, wegen der Möglichkeit aufeinanderfolgender Feiertage von höchstens 72 Stunden (vgl. § 6b Abs. 5 BDSG), die Pflicht zur Kennzeichnung der Videoüberwachung nach § 6b Abs. 2 BDSG und die grundsätzliche Unzulässigkeit von Videoüberwachung in Umkleide- und Sanitärbereichen.

Von Datenschutzaufsichtsbehörden anderer Länder war dem Landesbeauftragten bekannt geworden, dass gegenüber dortigen Einzelhändlern von ihren Sachversicherern mehrfach die Forderung nach Videoüberwachung des Geschäftes erhoben worden sei. Der Landesbeauftragte ist jedoch der Auffassung, dass eine Auflage der Versicherungswirtschaft, insbesondere im Einzelhandel Videoüberwachung zu betreiben, keine Auswirkung auf die Zulässigkeitsprüfung nach § 6b BDSG haben kann. Dies gilt auch dann, wenn der verantwortlichen Stelle im Fall der Installation einer Videoüberwachungsanlage eine niedrigere Versicherungsprämie angeboten wird. Allenfalls bei der Prüfung des berechtigten Interesses der verantwortlichen Stelle könnte dies unter Umständen berücksichtigt werden.

15.2.4 Videoüberwachung in Restaurants

Bürgerinnen und Bürger haben das Recht, den Besuch von Gaststätten unbeobachtet zu genießen (vgl. XI. Tätigkeitsbericht, Nr. 4.17.4). Da die Besucherbereiche gastronomischer Einrichtungen in der Regel zum öffentlich zugänglichen Raum im Sinne des BDSG zählen, ist dort eine Videoüberwachung nur unter den Voraussetzungen des § 6b BDSG möglich. Durch die Möglichkeit für die Gäste, sich längere Zeit dort aufzuhalten, Speisen und Getränke zu verzehren und mit Dritten ungezwungen zu kommunizieren, bestehen in rechtlicher Hinsicht enge Grenzen, die Gastbereiche per Video zu überwachen. In der Regel werden zumindest Anhaltspunkte dafür sprechen, dass die schutzwürdigen Interessen der betroffenen Gäste gegenüber den wie auch immer motivierten Interessen des Betreibers überwiegen (§ 6b Abs. 1 BDSG).

Gleichwohl ist dem Landesbeauftragten durch die Beschwerde eines Gastes bekannt geworden, dass der Betreiber eines beliebten Restaurants die ca. 40 Tische und weitere Gastbereiche des Freigeländes permanent mittels mehrerer Kameras überwachte. Es gab eine ganze Reihe berechtigter Interessen, diese Bereiche des Restaurants außerhalb der Öffnungszeiten per Video zu überwachen: Einbrüche, Sachbeschädigungen oder Diebstähle sollten dokumentiert und daraus folgende Schäden entsprechend geltend gemacht werden.

Im Rahmen der Sachverhaltsaufklärung war nicht ermittelbar, ob der Kamerabetreiber die Mühen gescheut hatte, die Videoüberwachung ausschließlich auf die Schließzeiten seines Restaurants zu beschränken, oder ob nicht doch die Kontrolle des eigenen Servicepersonals hinter der Rundumüberwachung steckte. Jedenfalls musste der zunächst beratungsresistenten Restaurantgeschäftsführung erst ein empfindliches Zwangsgeld angedroht werden, ehe überhaupt Auskunft erteilt und dann die Videoüberwachung der Gastbereiche auf die Zeiten außerhalb der Öffnungszeit reduziert wurde. Die berechtigten Interessen des Restaurantbetreibers überwiegen gegenüber den Interessen von Personen, die sich außerhalb der Öffnungszeiten unbefugt auf dem Restaurantgelände aufhalten könnten.

15.2.5 Videoüberwachung in Spielbanken

Kurz vor Jahresende 2014 wurde in Sachsen-Anhalt eine Spielbank eröffnet. Der Landesbeauftragte begleitete die Planungen des Betreibers bereits vor der Eröffnung und in vielerlei Hinsicht.

Zunächst war der Einsatz eines Venenscanners zum Zwecke der Einlasskontrolle im Gespräch. Angesichts der besonderen Sensibilität biometrischer Daten verwarf der Betreiber dieses Vorhaben nach Beratung durch den Landesbeauftragten. Ebenfalls zur Einlasskontrolle und zum Führen der Besucherdatei war beabsichtigt, die Personalausweise der Gäste zu kopieren bzw. einzuscannen. Nachdem der Landesbeauftragte diesbezüglich erhebliche datenschutzrechtliche Bedenken äußerte (vgl. Nr. 14.6), nahm der Betreiber auch hiervon Abstand.

Die weiteren Erörterungen galten der geplanten Videoüberwachung in der Spielbank. Die Besonderheit bestand darin, dass für den weitaus größten Teil der Spielbank Videoüberwachung gesetzlich vorgeschrieben ist. Nach § 8 SpielbG LSA sind zur Überwachung der Ermittlung des Bruttospielertrages und der Tronceinnahmen, zur Sicherstellung des ordnungsgemäßen Spielablaufs und zum Schutz der Spielbankbesucher technische Mittel zur Anfertigung von Bildaufzeichnungen einzusetzen. Dies betrifft die zur Spielbank gehörenden Eingangsbereiche für Besucher und Personal, die Rezeptions- und Kassenbereiche, die Spielsäle, die einzelnen Spieltische, sowie die Abrechnungsräume und internen Sicherheitsbereiche der Spielbank. Die Prüfung, ob diese Videoüberwachungsanlage entsprechend der gesetzlichen Vorgaben installiert ist und dabei auch die schutzwürdigen Interessen der Betroffenen gewahrt bleiben, obliegt dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt als dem für Spielbankaufsicht zuständigen Ministerium und Genehmigungsbehörde. Die entsprechende Bewertung durch das Ministerium hat der Landesbeauftragte beratend unterstützt.

Die Videoüberwachung der Spielbank sollte nach dem Willen des Betreibers jedoch über den gesetzlichen Pflichtumfang hinausgehen. Geplant war zunächst, dass die

Außenbereiche inklusive der Parkflächen, eine Außenterrasse mit gastronomischer Versorgung, Flure und ein Schulungsraum im Verwaltungstrakt, Lager-, Werkstatt- und Küchenräume sowie die Vorräume zu den Gästetoiletten mit insgesamt 38 Videokameras rund um die Uhr erfasst und die Aufnahmen für die Dauer von zwei Wochen gespeichert werden.

Dieser Teil der Videoüberwachung ist nach den Vorgaben des BDSG zu bewerten. Der Landesbeauftragte hat dabei die Intention des Betreibers berücksichtigt, Gefahren für Gäste und Beschäftigte sowie ihr Eigentum und das Eigentum der Spielbank abzuwehren oder auch Beweise bei entsprechenden dennoch stattfindenden schädigenden Handlungen zu sichern. Gleichwohl war zu begrüßen, dass der Betreiber den geäußerten datenschutzrechtlichen Bedenken Rechnung trug, indem er bereits weitestgehend auf die Kamerainstallationen auf der gastronomischen Außenterrasse, im Schulungs- und einem Lagerraum sowie in den Vorräumen zu den Toiletten verzichtete. Zudem hat der Betreiber den schutzwürdigen Interessen der betroffenen Beschäftigten Rechnung getragen, indem er auf die Ausrichtung der Kameras auf Dauerarbeitsplätze von Technikern sowie die rein präventive Überwachung durch zwei Kameras wegen befürchteter Diebstähle aus Küchenvorratsräumen verzichtete. Beides hatte der Landesbeauftragte zuvor im Lichte des § 32 BDSG als unzulässig bewertet. Zudem bestand Einvernehmen, dass die Speicherfrist von bis zu zwei Wochen, die § 8 Abs. 4 SpielbG LSA vorgibt, für die verbliebenen 26 Videokameras, die nach BDSG zu bewerten sind, keine Anwendung finden kann, sondern eine kürzere Speicherfrist von maximal 48 Stunden vorzusehen ist.

Da der Betreiber avisiert, baldmöglichst eine weitere Spielbank an einem anderen Standort in Sachsen-Anhalt zu eröffnen, wird diese Thematik den Landesbeauftragten vermutlich auch im nächsten Berichtszeitraum beschäftigen.

15.2.6 Videoüberwachung in Taxis

Bereits in seinem XI. Tätigkeitsbericht (Nr. 4.17.5) hatte der Landesbeauftragte darauf hingewiesen, dass eine große Taxigenossenschaft die Ausstattung ihrer Wagen mit Innenraumkameras plane. Mehrfach wurde die Genossenschaft darauf hingewiesen, dass der Taxiinnenraum als öffentlich zugänglich zu betrachten ist und daher die Voraussetzungen des § 6b BDSG einzuhalten sind. Dies schließe anlasslose und permanente Videoüberwachungen aus. Ein berechtigtes Interesse könne allerdings z. B. bei Angriffen gegen die Fahrer vorliegen. Dann wäre aber zunächst zu prüfen, ob andere Mittel nicht mindestens genauso geeignet sind, Angriffe einzuschränken bzw. die Täter zu stellen. In Betracht zu ziehen wären z. B. die Möglichkeit der Auslösung eines „stillen Alarms“, eines GPS-gestützten Notrufsignals oder der Anfertigung eines Standbildes. Letztere Mittel seien bei gleicher Eignung vorzugswürdig, da ihr Einsatz nicht mit einer Permantentüberwachung des Fahrgastverhaltens verbunden ist.

Nachdem der Landesbeauftragte seine Rechtauffassung dargelegt hatte, teilte ihm die Genossenschaft mit, dass eine Videoüberwachung nicht durchgeführt und er bei Veränderungen informiert werde.

15.2.7 Dashcams

Die Dashcam, also die Kamera auf dem Armaturenbrett eines Autos, erfreut sich zunehmender Beliebtheit. Die kleine Kamera sieht, was der Fahrer sieht, und zeichnet es auf. Auf der eingesteckten SD- oder MicroSD-Karte mit bis zu 64 GB werden schon längst nicht mehr lediglich einzelne Fotos, sondern hochaufgelöste Videobilder gespeichert. Die Aufnahmen können auf PCs betrachtet und weiterbearbeitet werden.

Dashcamaufnahmen, gefertigt mit dem Ziel, einen möglichen Unfallhergang zu dokumentieren und die Aufnahmen zum Nachweis der eigenen Unschuld der Polizei zu übergeben oder als Beweismittel in einem zivilrechtlichen Schadenersatzprozess zu verwenden, haben eine gewichtige datenschutzrechtliche Komponente: Mit einer Dashcam werden regelmäßig andere Verkehrsteilnehmer fortlaufend erfasst, auch diejenigen, die nicht an Unfällen beteiligt sind, und die ohnehin keine Kenntnis von der Beobachtung haben und sich daher dieser nicht entziehen können.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten mithilfe einer Dashcam im öffentlichen Verkehrsraum stellt eine Videoüberwachung im Sinne von § 6b BDSG dar. Die Tatsache, dass die Aufnahmen oft von Privatpersonen angefertigt werden, ändert daran nichts. Zwar ist das BDSG gemäß § 1 Abs. 2 Nr. 3 nicht anwendbar, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ausschließlich für persönliche oder familiäre Zwecke erfolgt. In seinem Urteil vom 11. Dezember 2014 (Az. C212/13, siehe Nr. 15.2.2) wies der Europäische Gerichtshof jedoch darauf hin, dass eine Videoüberwachung öffentlichen Raumes keine Videoüberwachung ist, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.

Sehr fraglich ist, ob der Zweck, die Videoaufnahmen als Beweismittel zu verwenden, erreicht werden kann. Das Amtsgericht München hatte entschieden, dass Dashcam-Aufzeichnungen im Zivilprozess nicht als Beweismittel verwertet werden können (Urteil vom 13. August 2014, Az. 345 C 5551/14, juris). Das Landgericht Heilbronn schloss sich mit Urteil vom 17. Februar 2015 (Az. I 3 S 19/14, juris) dieser Beurteilung an, da diese Aufnahmen in aller Regel unter Verletzung des Grundrechts der Betroffenen auf informationelle Selbstbestimmung gewonnen werden. Doch die Rechtsprechung ist z. Z. noch nicht einheitlich: Das Amtsgericht Nienburg hatte mit Urteil vom 20. Januar 2015 (Az. 4 Ds 520 Js 39473/14 (155/14), juris) die Aufnahmen einer Dashcam in einem Einzelfall im Strafverfahren als gerichtsverwertbar angesehen.

Doch selbst wenn im Einzelfall die Videoaufnahmen als Beweismittel zugelassen werden, bergen sie Risiken für die verantwortliche Stelle. In einem Zivilverfahren vor dem Amtsgericht München bezog sich ein Radfahrer zum Beweis seiner Unschuld an einem Verkehrsunfall auf ein von ihm selbst gefertigtes Video. Nach Auswertung ging das Gericht allerdings von einem überwiegenden Verschulden des Radfahrers aus (Urteil vom 6. Juni 2013, Az. 343 C 4445/13, juris).

Außerdem ist bei der Verwendung einer Dashcam das Recht der Betroffenen am eigenen Bild zu beachten. Dieses Recht ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts, bei dessen Verletzung zivilrechtliche Unterlassungs- und Schadensersatzansprüche geltend gemacht werden können (vgl. Nr. 15.2.1).

Sein Schutzbereich ist bereits eröffnet, wenn ein Bildnis ohne die Einwilligung des Abgebildeten angefertigt wird, selbst wenn dies nicht mit der Absicht geschieht, das Bild zu veröffentlichen oder zu verbreiten und selbst dann, wenn der Abgebildete gerade eine Ordnungswidrigkeit begeht. Das Amtsgericht Bonn (Urteil vom 28. Januar 2014, Az. 109 C 228/13, juris) kommt daher im Rahmen der Rechtsgüterabwägung zu der Feststellung, dass die schutzwürdigen Interessen der Betroffenen am Nichtüberwachtwerden, und sei die Überwachung auch nur kurzzeitig, den berechtigten Interessen der verantwortlichen Stelle überwiegen. Diese Sichtweise vertritt im Übrigen auch der Düsseldorfer Kreis in seinem Beschluss vom 25. bis 26. Februar 2014 zur Unzulässigkeit der Videoüberwachung aus Fahrzeugen (**Anlage 37**).

Die datenschutzrechtliche Brisanz des Betriebes von Dashcams haben einige Hersteller bereits erkannt und versuchen gegenzusteuern. Es sind inzwischen Kameras auf dem Markt, die nur die letzten 15 gesehenen Sekunden aufzeichnen und länger zurückliegende Bildsequenzen automatisch überschreiben. Erst bei einer starken Erschütterung, z. B. einem Aufprall, unterbleibt die automatische Löschung. Nach Meinung des Landesbeauftragten liegt auch in diesem Fall eine Videoüberwachung im Sinne von § 6b BDSG vor.

Der Deutsche Verkehrsgerichtstag empfahl auf seiner Tagung im Januar 2016, den Umfang der Verwendung von Dashcams und Verwertung entsprechender Aufnahmen durch Gesetz klarzustellen.

15.2.8 Videoüberwachung in öffentlichen Verkehrsmitteln

Auch in öffentlichen Verkehrsmitteln sind Videokameras inzwischen weit verbreitet. Die Ausstattung der Fahrzeuge mit entsprechender Technik nimmt zu. Der Einsatz dient nach dem Willen der Aufgabenträger und Verkehrsunternehmen in der Regel der Sicherheit der Fahrgäste und des Personals sowie dem Schutz des Eigentums der Verkehrsunternehmen. Dieses durchaus berechtigte Ziel kann gleichwohl nicht ohne nähere Prüfung eine häufig fast flächendeckende Videoüberwachung rechtfertigen. Hierzu bedarf es wiederum einer Detailbetrachtung, die die schutzwürdigen Interessen der Betroffenen, die in der Regel überwiegend keinen Anlass für eine Überwachung geben, angemessen berücksichtigt.

Im Tätigkeitszeitraum haben es sich daher die Datenschutzaufsichtsbehörden in der Arbeitsgruppe Videoüberwachung zur Aufgabe gemacht, aktuelle Hinweise für einen datenschutzgerechten Einsatz von optisch-elektronischen Einrichtungen in öffentlichen Verkehrsmitteln zu erarbeiten. Diese Orientierungshilfe soll den rechtlichen Rahmen aufzeigen, der sich aus der Anwendung der Vorschriften des BDSG, insbesondere §§ 6b und 32 BDSG, ergibt, und richtet sich somit vornehmlich an Verkehrsbetriebe, die nicht öffentlich-rechtlich organisiert sind.

Allerdings kann die Orientierungshilfe auch den öffentlich-rechtlichen Aufgabenträgern – dies sind die Länder, Landkreise und kreisfreien Städte – den Rahmen aufzeigen, innerhalb dessen Videoüberwachung in öffentlichen Verkehrsmitteln zulässig betrieben werden kann. Für die Aufgabenträger ist dies bereits relevant, wenn sie im Rahmen einer Ausschreibung von Verkehrsleistungen die Anforderungen formulieren, die sie an die bietenden Verkehrsunternehmen stellen, bzw. wenn sie entsprechende vertragliche Regelungen erarbeiten.

Die Hinweise in der Orientierungshilfe reichen von Umfang und technischer Ausgestaltung einer zulässigen Videoüberwachung über die zu beachtenden schutzwürdigen Interessen und Rechte der Fahrgäste und Beschäftigten der Verkehrsunternehmen bis hin zu den notwendigen organisatorischen Rahmenbedingungen einschließlich der Voraussetzungen für eine Übermittlung der Videoaufnahmen an Polizei und Staatsanwaltschaft.

Der Landesbeauftragte wird, da die Erörterungen um die Orientierungshilfe abgeschlossen sind, die abgestimmten Hinweise gegenüber Verkehrsunternehmen und Aufgabenträgern in Sachsen-Anhalt kommunizieren und verstärkt darauf hinwirken, dass die rechtlichen Vorgaben in der Praxis auch künftig Beachtung finden. Die Orientierungshilfe ist auf der Homepage des Landesbeauftragten abrufbar.[12]

Davon unabhängig erreichten den Landesbeauftragten Eingaben hinsichtlich eines Verkehrsunternehmens mit Sitz in Sachsen-Anhalt, in denen sich einzelne Beschäftigte und der Betriebsrat über die Nutzung von Videoaufnahmen zur Verhaltens- und Leistungskontrolle von Beschäftigten (vgl. hierzu auch Nr. 15.2.10) beschwerten. Der Landesbeauftragte hat zunächst das Verkehrsunternehmen um Stellungnahme zu diesen Vorwürfen gebeten. Dabei wird er insbesondere prüfen, ob die Videoaufnahmen entgegen § 6b Abs. 3 BDSG zu einem nicht zuvor festgelegten Zweck (hier: Verfolgung von Schädigern in Verkehrsmitteln) verarbeitet oder genutzt wurden.

15.2.9 Kfz-Kennzeichenerfassung in Parkhäusern

Bereits seit 1994 ist auf deutschen Kfz-Kennzeichen eine besondere Schriftart zu verwenden. Es handelt sich um eine FE-Schrift, also um eine fälschungserschwerende Schrift. Die damals neue Schriftart hatte jedoch noch einen weiteren Zweck: Sie sollte ihre leichte Maschinenlesbarkeit gewährleisten. Diese Eigenschaft hatte in den letzten Jahren eine datenschutzrechtlich beachtenswerte Dimension erhalten: In Parkhäusern werden vermehrt automatische Kennzeichenerfassungssysteme eingesetzt. Dabei werden aus Videosequenzen oder Fotografien der ein- und ausfahrenden Fahrzeuge mittels Texterkennung die Kennzeichen extrahiert und gespeichert.

Das Kennzeichen eines Kfz stellt nach herrschender Meinung ein personenbeziehbares Datum des Kfz-Halters dar. Die Erhebung und Speicherung der Kennzeichen durch Parkhausbetreiber wird in der Regel nicht erforderlich und damit nicht zulässig sein. Ausfahren darf nur, wer die Parkgebühr bezahlt hat. Das funktioniert auch anonym.

Jedoch sind auch Szenarien vorstellbar, in denen die Erhebung und Verarbeitung der Kfz-Kennzeichen begründbar wäre: Wenn z. B. ein Cabrio-Besitzer im Herbst seinen Wagen in einem öffentlichen Parkhaus abstellt, im nächsten Frühjahr wieder abholt und dabei glaubhaft zu machen versucht, sein eintägiges Parkticket sei verloren gegangen und er wolle nun – leider – die volle Tagesgebühr bezahlen. Häufen sich solche Fälle bösgläubiger Kostendämpfung bei den Parkgebühren durch die Kunden, könnte dies durchaus erheblichen wirtschaftlichen Schaden für den Parkhausbetreiber verursachen. Kann der Parkhausbetreiber in einer solchen Situation den eingetretenen wirtschaftlichen Schaden belegen und sind auch künftig weitere wirtschaftli-

[12] http://lsaurl.de/VideoOEPNVOH

che Beeinträchtigungen zu erwarten, könnte nach Ansicht des Landesbeauftragten eine Speicherung der Kfz-Kennzeichen zur Kontrolle der ordnungsgemäßen Vertragsdurchführung geeignet, erforderlich, angemessen und somit rechtlich zulässig sein.

Der Landesbeauftragte hat in Beratungen auch auf den Aspekt der Speicherdauer der Kfz-Kennzeichen hingewiesen: Der Betreiber hätte die Kennzeichen der Fahrzeuge dann sofort zu löschen, wenn ihre weitere Speicherung für die Erfüllung des Zwecks nicht mehr erforderlich ist. Das wäre in der Regel mit dem Verlassen des Parkhauses der Fall. Der Betreiber würde also lediglich über eine Liste mit den Kennzeichen inklusive Datum und Uhrzeit der Einfahrt der Fahrzeuge verfügen, die sich aktuell in seinem Objekt befinden.

Es mag aus technischen Gründen vorstellbar sein, dass eine Datenlöschung nicht unmittelbar nach der Ausfahrt eines Fahrzeuges erfolgt. Der Landesbeauftragte würde aber eine Speicherdauer, die wesentlich über fünf Minuten nach Ausfahrt des Fahrzeuges hinausgeht, für jedenfalls datenschutzrechtlich problematisch ansehen und kritisch hinterfragen.

Außerdem hält der Landesbeauftragte aus rechtlichen Gründen eine differenzierte Betrachtung zwischen Kurzzeit- und Dauerparkern für notwendig, die freilich Herausforderungen in der praktischen Umsetzung birgt. Bei Dauerparkern wäre es nicht erforderlich, bei jedem Ein- und Ausfahrvorgang eine Bildaufnahme zu fertigen und das Kfz-Kennzeichen auszulesen. Vorzugswürdig wäre eine parallele Transponder- oder Kartenlösung, bei der die Benutzung des Transponders oder der Karte bestenfalls die Foto- bzw. Videoaufnahme in Gänze, mindestens aber die weitere Speicherung des Fotos, der Videosequenz und/oder des ggf. erkannten Kennzeichens verhindert. Bei Neubauten oder größeren Umbauten von Parkhäusern sollte dies im Rahmen des Privacy by Design bereits vorgesehen werden.

In jedem Fall wird bei Vorliegen einer Kfz-Kennzeichenerfassung neben der obligatorischen Erkennbarmachung der Videoüberwachung nach § 6b Abs. 2 BDSG auch ein Hinweis auf die Kennzeichenerfassung angezeigt sein, und zwar so rechtzeitig, dass Fahrzeugführer, die diese Art der Erhebung und Verarbeitung ihrer personenbezogenen Daten nicht wünschen, noch eine realistische Möglichkeit haben, vor der Einfahrt in den überwachten Bereich zu wenden.

15.2.10 Videoüberwachung der Beschäftigten

Bereits im XI. Tätigkeitsbericht (Nr. 4.17.3) ist ausgeführt, unter welch engen Voraussetzungen eine Videoüberwachung im Unternehmen zulässig ist, wenn von ihr auch Beschäftigte betroffen sind. Auch im hiesigen Berichtszeitraum war wieder eine erhebliche Zahl an Eingaben von (ehemaligen) Beschäftigten zu bearbeiten, die an ihrem Arbeitsplatz einer Videoüberwachung ausgesetzt sind oder waren.

Dabei ist auffällig, dass der klassische Anwendungsfall nicht der des § 32 BDSG ist, denn eine Videoüberwachung wird nur in den seltensten Fällen zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sein, und auch der konkrete Verdacht einer Straftat, wegen derer eine Videoüberwachung zur Aufklärung unvermeidbar war, lag in der Regel nicht vor. Vielmehr sind es häufig Gründe, die nicht in den Beschäftigten selbst liegen, die die Arbeitgeber zu einer Vi-

deoüberwachung veranlassen. So geht es z. B. häufig um die Überwachung oder Verbesserung von Betriebsabläufen, um die Abwehr von Gefahren, die von außen befürchtet werden, etwa durch Einbruch oder Diebstahl durch Firmenexterne, oder auch um Beweissicherung, um damit eigene Schadensersatzansprüche zu unterlegen oder unberechtigte Haftungsansprüche Dritter abzuwehren.

In diesen Fällen werden die Beschäftigten, auch wenn dies vordergründig nicht bezweckt ist, gleichwohl zu Betroffenen. Befindet sich dann auch noch ein Dauerarbeitsplatz von Beschäftigten im Erfassungsbereich einer Videokamera, ist eine besonders intensive Prüfung erforderlich, ob hier nicht schutzwürdige Interessen der Betroffenen gegenüber den berechtigten Interessen der Arbeitgeber überwiegen (vgl. §§ 6b Abs. 1, 28 Abs. 1 BDSG). Denn an ihren Arbeitsplätzen können Beschäftigte einer Videoüberwachung häufig nicht ausweichen. Und auch an der Wirksamkeit einer Einwilligung der Beschäftigten in die Datenverarbeitung sind häufig Zweifel angebracht, da es angesichts des Abhängigkeitsverhältnisses gegenüber dem Arbeitgeber an der Freiwilligkeit mangeln dürfte (§ 4a Abs. 1 Satz 1 BDSG).

Nach der ständigen Rechtsprechung des Bundesarbeitsgerichtes ist bei der Überwachung von Beschäftigten ein besonders strenger Maßstab anzuwenden (vgl. bereits Urteil vom 7. Oktober 1987, Az. 5 AZR 116/86, NZA 1988, 92; zuletzt auch Urteil vom 21. November 2013, Az. 2 AZR 797/11, BAGE 146, 303). Eine dauerhafte Mitarbeiterüberwachung darf wegen des ständigen Überwachungsdrucks wenn überhaupt dann nur äußerst restriktiv eingesetzt werden. Denkbar ist dies etwa im Einzelhandel, in dem eine Videoüberwachung zur Senkung einer signifikanten Diebstahlsquote in den Verkaufsräumen im Einzelfall als arbeitsplatzimmanent einzustufen sein kann. Generell unzulässig ist es, die Bereiche zu überwachen, die Beschäftigte in ihren Pausen zur Entspannung und Kommunikation nutzen oder die der persönlichen Intimsphäre zuzurechnen sind; das sind insbesondere Aufenthalts-, Umkleide- und Sanitärräume. Eine Verhaltens- und Leistungskontrolle durch Videoüberwachung ist ebenso, auch in Verkaufsräumen, unzulässig.

Der Landesbeauftragte hat in den im Berichtszeitraum bearbeiteten Einzelfällen zunächst erörtert, ob es mildere Mittel gibt, mit denen die Arbeitgeber ihre Ziele erreichen können. Eine Überprüfung von Betriebsabläufen sollte in erster Linie durch eine reine Sichtkontrolle des Ablaufes oder des Endproduktes ohne technische Hilfsmittel oder durch die Analyse von Unternehmenskennzahlen möglich sein. Der Einbruchs- oder Diebstahlsgefahr kann ggf. bereits durch andere Sicherungsmaßnahmen begegnet werden, wie Umzäunungen, Sicherheitspersonal, einbruchhemmende Fenster und Türen, Sicherheitsschlösser, Zugangssicherungen.

Ferner hat der Landesbeauftragte untersucht, ob im Sinne der Datensparsamkeit zunächst eine Einschränkung der Überwachungsmaßnahme möglich ist, ohne die berechtigten Interessen der Arbeitgeber zu gefährden. In dem Fall eines Autohauses etwa fand u. a. eine Live-Beobachtung der gesamten Werkstatt mit den Hebebühnen durch den Geschäftsführer statt. Hier konnte der Landesbeauftragte erreichen, dass die Bildbereiche von Dauerarbeitsplätzen oder üblichen Arbeitsbereichen unkenntlich gemacht wurden.

Des Weiteren war an eine Neuausrichtung der Kameraeinstellung zu denken, z. B. in einem vom Landesbeauftragten behandelten Fall eines Produktionsbetriebes. In diesem sollten mit der Videoüberwachung u. a. mögliche Störungen auf einem Trans-

portband frühzeitig erkannt werden. Das Unternehmen arbeitet derzeit daran, die Kamera sehr eingeschränkt nur auf dieses Transportband auszurichten, sodass von den dort Beschäftigten allenfalls die (behandschuhten) Hände erfasst werden.

Sofern sich die Einbruchs- und Diebstahlsgefahr etwa besonders auf die Zeitfenster außerhalb der üblichen Geschäftszeiten beschränkte, wirkte der Landesbeauftragte stets darauf hin, die Videokameras während des Geschäftsbetriebes zu deaktivieren.

Nicht zuletzt sollte auch bedacht werden, dass sich aus der Verletzung von Persönlichkeitsrechten auch zivil- und arbeitsrechtliche Abwehr- und Entschädigungsansprüche ergeben können. Für den Fall der nahezu stets unzulässigen heimlichen Videoüberwachung von Beschäftigten etwa hat das Bundesarbeitsgericht jüngst seine entsprechende Rechtsprechung fortgesetzt. Es bestätigte einen Geldentschädigungsanspruch (hier: Schmerzensgeld) einer Beschäftigten, die im Krankheitsfall durch Detektive im Auftrag ihres Arbeitgebers videoüberwacht worden war, um die Umstände der Krankheit zu überprüfen (Urteil vom 19. Februar 2015, Az. 8 AZR 1007/13, juris).

Neben den materiellen Fragen durfte die Prüfung des Landesbeauftragten auch Fragen der Organisation und des Verfahrens nicht außer Acht lassen. Längst nicht jedes Unternehmen führte das gesetzlich vorgeschriebene Verfahrensverzeichnis (vgl. § 4g Abs. 2 und 2a BDSG), in dem die verantwortliche Stelle die Zwecke und Ausgestaltung der Videoüberwachung konkret festzulegen hat und das auf Antrag jedermann zur Verfügung zu stellen ist.

Besonders bei umfangreichen Videoüberwachungsmaßnahmen ist zu prüfen, ob sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dann nämlich ist eine besondere Prüfung vor Beginn der Videoüberwachung durchzuführen und zu dokumentieren, die sog. Vorabkontrolle (§ 4d Abs. 5 BDSG). Auf diese wirkte der Landesbeauftragte insbesondere bei umfassenden Videoüberwachungsanlagen hin, etwa in einer Spielbank (vgl. Nr. 15.2.5) oder im Einzelhandel (vgl. Nr. 15.2.3). Die Vorabkontrolle führt der betriebliche Beauftragte für den Datenschutz durch, der in diesen Fällen zwingend zu bestellen ist (§§ 4d Abs. 6, 4f Abs. 1 Satz 6 BDSG).

Letztlich hat – sofern vorhanden – die Arbeitnehmervertretung mitzubestimmen, wenn es um Einführung und Anwendung von technischen Einrichtungen geht, die es ermöglichen, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG in der Auslegung des Bundesarbeitsgerichtes, vgl. bereits Beschluss vom 6. Dezember 1983, Az. 1 ABR 43/81, BAGE 44, 285 und daran anschließende Entscheidungen; vgl. auch §§ 32 Abs. 3 BDSG, 75 Abs. 2 BetrVG).

15.2.11 Webcams

Der Landesbeauftragte hatte in seinem XI. Tätigkeitsbericht (Nr. 4.17.7) ausführlich über die datenschutzrechtlichen Risiken eines Webcam-Betriebes berichtet und Empfehlungen zum datenschutzgerechten Einsatz von Webcams gegeben. Gleichwohl gingen im aktuellen Berichtszeitraum wieder Beschwerden Betroffener über solche Kameras ein. Mithilfe einer Webcam im Internet dargestellte Orte können ganz trivial der Marktplatz einer touristisch interessanten Stadt oder auch der Zugang

zu einer Bäckerei, aber auch der Eingangsbereich zu Hotels oder zu einer auf Scheidungsrecht spezialisierten Anwaltskanzlei sein.

Bei der Bearbeitung der Beschwerden war stets die Frage relevant, ob durch Webcam-Aufnahmen, die ins Internet eingestellt werden, für einen Dritten, z. B. dem Nachbarn, bekannte Personen wiedererkennbar waren, sie also identifiziert werden konnten. War dies der Fall, enthielten die Aufnahmen personenbezogene Daten i. S. v. § 3 Abs. 1 BDSG. Ob der Betreiber einer Webcam als verantwortliche Stelle selbst zu einer Identifizierung in der Lage ist, er sie anstrebt oder sie nur Nebenfolge des eigentlich Gewollten ist, ist dabei unerheblich. Erst wenn die Anonymität der möglicherweise aufgezeichneten Personen gewährleistet ist, fehlt es hier an der Erhebung von personenbeziehbaren Daten (vgl. Verwaltungsgericht Schwerin, Beschluss vom 18. Juni 2015, Az. 6 B 1637/15 SN, juris).

Sind natürliche Personen identifizierbar, ist auf Webcams, die öffentlich zugängliche Bereiche ablichten, § 6b BDSG anwendbar. Die Videoüberwachung wäre dann nur zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Abgelichteten überwiegen. Ob die Darstellung des aktuellen Geschehens auf einem touristisch interessanten Platz oder einem Verkehrsknotenpunkt in einer Großstadt ein berechtigtes Interesse darstellen kann, erscheint schon fraglich. Jedenfalls dürften in aller Regel Anhaltspunkte dafür bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Das Überwiegen der schutzwürdigen Interessen muss nicht zwangsläufig positiv festgestellt werden. Es reicht aus, wenn Anhaltspunkte für das Überwiegen schutzwürdiger Interessen nicht ausgeräumt werden können. Dies kann regelmäßig angenommen werden, wenn öffentliche Bereiche permanent abgelichtet und die Aufnahmen ins Internet eingestellt werden. Der Eingriff in die Persönlichkeitsrechte in diesen Fällen ist erheblich, da weltweit festgestellt werden kann, wer wie gekleidet sich in welcher Begleitung in dem betreffenden Bereich bewegt. Mit in die Abwägung einbezogen werden muss auch, dass es jedem Dritten vollständig überlassen bleibt, wie er mit diesen Videoaufnahmen verfährt, ob er sie auswertet, speichert oder weiterverarbeitet, ohne dass die Betroffenen oder die verantwortliche Stelle darüber etwas erfahren (vgl. Verwaltungsgericht Schwerin, a. a. O.). Denn gegen einen Missbrauch der Webcam-Aufnahmen gibt es kaum ein wirksames Mittel, was viele Beispiele auf Videostreamingdiensten wie „YouTube“ zeigen (vgl. Scholz, in: Simitis, BDSG, 8. Auflage, 2014, § 6b Rn. 122). Entsprechend gewichtige Interessen auf Seiten des Webcam-Betreibers sind kaum ersichtlich. Mitunter reichen geringe Korrekturen der Qualität der Aufnahmen aus, um die Identifizierung zu verhindern. Das Ziel der Webcam-Aufnahmen, das Geschehen an einem markanten Ort zu präsentieren, kann gleichwohl erreicht werden.

Der Landesbeauftragte hat stets darauf hingewirkt, die Kameraausrichtung und Bildauflösung so aufeinander abzustimmen, dass auf den veröffentlichten Aufnahmen Personen oder sie identifizierende Gegenstände, wie z. B. Fahrzeuge, auch unter Berücksichtigung von Weiterverarbeitungsmöglichkeiten nicht erkennbar sind.

15.2.12 Drohnen

Anlässlich der Feldtage der Deutschen Landwirtschafts-Gesellschaft im Jahr 2014 in Bernburg hat sich der Landesbeauftragte mit der Frage der Zulässigkeit von Video-

überwachung aus der Luft befasst. An dem dortigen Infozentrum „Das Wissen kommt von oben – Drohnen und Fernerkundungssysteme in der Landwirtschaft“ konnten sich Besucher über den Stand der Technik und die verschiedenen Einsatzgebiete informieren. Für den Landesbeauftragten stellt sich angesichts der Entwicklung und Verbreitung dieser Technik allgemein die Frage, unter welchen Bedingungen deren Einsatz datenschutzrechtlich zulässig ist.

Drohnen sind der umgangssprachliche Begriff für unbemannte Luftfahrzeuge, die ohne eine an Bord befindliche Besatzung automatisiert oder durch einen Menschen über eine Fernsteuerung betrieben und navigiert werden können.

Die Einsatzgebiete sind vielfältig. Im Bereich der zivilen Nutzung durch nicht-öffentliche Stellen ist dabei etwa an die Erkundung unzugänglicher Gebiete, Begutachtung von Witterungs- und Brandschäden auf großen Flächen, dies z. B. in der Land- und Forstwirtschaft, aber auch die technische Kontrolle, etwa bei Hochspannungsanlagen und Bauwerken, zu denken. Besonders der Einsatz zur Paketauslieferung wurde zuletzt intensiv medial begleitet. Zunehmender Beliebtheit erfreuen sich Drohnen zudem im Freizeitbereich als reines Hobby-Objekt. Die Presse berichtete, sie seien im Weihnachtsgeschäft 2014 das Trendgeschenk schlechthin gewesen. Die Preise für einfache Modelle sinken stetig, weshalb die Absatzzahlen steigen. Den meisten Nutzungen ist dabei immanent, dass die Fluggeräte bestenfalls oder sogar notwendig mit Foto- oder Videotechnik ausgestattet sind.

Zunächst ist zu beachten, dass der Einsatz unbemannter Fluggeräte auch den luftverkehrsrechtlichen Vorschriften unterfällt und erlaubnispflichtig sein kann. Dabei kommt es auf den Einsatzzweck an. Werden Drohnen zum Zwecke des Sports oder der Freizeitgestaltung genutzt, können sie bis zu einem Gewicht von 5 kg sowie einer Aufstiegshöhe von maximal 100 Metern und außerhalb eines Umkreises von 1,5 km rund um Flugplätze ohne Genehmigung betrieben werden.

Jeglicher Einsatz außerhalb dieses Rahmens bedarf einer behördlichen Aufstiegserlaubnis, innerhalb derer die zuständige Luftfahrtbehörde datenschutzrechtliche Aspekte berücksichtigen muss (vgl. § 1 Abs. 2 Satz 3 LuftVG, § 16 Abs. 1 LuftVO mit weiteren Abgrenzungsdetails, § 16 Abs. 4 Satz 1 LuftVO). Die datenschutzrechtliche Prüfung der Luftfahrtbehörde hinsichtlich des erlaubnispflichtigen Drohneneinsatzes kann der Landesbeauftragte bei Bedarf beratend unterstützen.

Bei der Nutzung zu Zwecken des Sports oder der Freizeitgestaltung mag die Vermutung naheliegen zu vermuten, dass diese rein private Nutzung eine ausschließlich persönliche oder familiäre Tätigkeit sein könnte, die nicht dem Anwendungsbereich des BDSG unterfällt (§ 1 Abs. 2 Nr. 3 BDSG). Allerdings ist auch hier die jüngste Rechtsprechung des Europäischen Gerichtshofes zu beachten (vgl. Nr. 15.2.2), wonach es sich nicht um eine ausschließlich persönliche oder familiäre Tätigkeit handeln kann, wenn öffentlich zugängliche Bereiche (mit-)erfasst werden. Dies dürfte beim Überflug einer größeren Fläche durch eine Drohne regelmäßig der Fall sein. Und auch wenn keine öffentlich zugänglichen Bereiche betroffen sind, aber der Videoflug dazu dient, den Nachbargarten auszukundschaften, wäre zu prüfen, ob die Maßnahme damit die rein persönliche und familiäre Sphäre des Drohnenbetreibers verlässt.

Daher haben die verantwortliche Stelle und der Landesbeauftragte, wenn ihm ein solcher Drohneneinsatz bekannt wird, stets anhand der Vorgaben des BDSG, insbesondere der §§ 6b und 28 BDSG zu prüfen, ob die Videoaufnahmen durch die Drohne zur Wahrnehmung berechtigter Interessen der verantwortlichen Stelle erforderlich sind und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Ob eine Videoaufnahme mittels einer Drohne allein zur Freizeitgestaltung dabei als berechtigtes Interesse anerkannt werden kann, ist zu bezweifeln. Jedenfalls dürfte bei einem solchen Einsatzzweck in der Regel das schutzwürdige Interesse der von der Videoüberwachung Betroffenen überwiegen, etwa der Nachbarn, die sich unbeobachtet auf ihren Grundstücken und den öffentlichen Straßen und Plätzen bewegen möchten.

In der Interessenabwägung wird stets auch zu berücksichtigen sein, dass ein Hinweis auf die Videoüberwachung und die verantwortliche Stelle, wie es § 6b Abs. 2 BDSG fordert, regelmäßig nicht möglich ist, dass die Betroffenen häufig nicht mit einer Videoaufnahme aus der Luft rechnen, die Überwachung also vielfach (zunächst) heimlich erfolgen dürfte, und dass, selbst wenn die Betroffenen die Video-Drohne bemerken, sie dem Erfassungsbereich nur bedingt ausweichen können. Die Abwägung dürfte damit in der Regel gegen die Videoüberwachung aus der Luft ausfallen.

Hinzu kommt, dass ein Betreiber, der mithilfe einer Drohne ein ansonsten nicht einsehbares Privatgrundstück aufnimmt oder einen nur aus der Luft möglichen Einblick in fremde Fenster wagt, damit derart in den höchstpersönlichen Lebensbereich und die Intimsphäre der Betroffenen eingreift, dass er sich nach § 201a StGB strafbar machen könnte. Die Betroffenen können sich auch zivilrechtlich zur Wehr setzen.

Der Landesbeauftragte rät daher, beim Einsatz von Video-Drohnen zur Freizeitgestaltung auf die Erfassung personenbezogener Daten Dritter, die sich nicht damit einverstanden erklärt haben, gänzlich zu verzichten.

Aber auch bei dem gewerblichen bzw. erlaubnispflichtigen Einsatz einer Video-Drohne ist Vorsicht geboten. Verstößt ein Betreiber in diesen Fällen gegen Datenschutzvorschriften, sind die Ordnungswidrigkeiten- und Straftatbestände der §§ 43 und 44 BDSG durch den Landesbeauftragten ebenso wie die des § 43 LuftVO durch die Luftfahrtbehörde zu prüfen und ggf. zu ahnden. Eine Aufstiegserlaubnis der Luftfahrtbehörde entbindet den Betreiber daher nicht von seiner Pflicht, bei jeder Nutzung stets die schutzwürdigen Interessen potenziell betroffener Personen angemessen zu berücksichtigen.

Der Düsseldorfer Kreis hat am 16. September 2015 einen Beschluss mit entsprechenden Hinweisen gefasst[13].

Um Gefährdungen im Luftraum und am Boden, z. B. durch Kollisionen oder Abstürze, zu vermindern, arbeitet das Bundesministerium für Verkehr und digitale Infrastruktur nach eigenen Angaben derzeit an Neuregelungen für den privaten und gewerblichen Einsatz von Drohnen. Auch die EU-Kommission und die EU-Verkehrsminister beschäftigen sich intensiv mit der luftverkehrs- und datenschutzrechtlichen

[13] http://lsaurl.de/PrivKamDro

Relevanz von Drohnen und arbeiten an EU-einheitlichen Vorgaben. Der Landesbeauftragte wird die weitere Entwicklung begleiten.

Nun wird es vermutlich häufig vorkommen, dass Betroffene über sich in der Luft eine möglicherweise mit Videotechnik ausgestattete Drohne feststellen, aber den Betreiber nicht ausfindig machen können. Zunächst einmal besteht die Möglichkeit, bei der zuständigen Luftfahrtbehörde anzufragen, ob eine Aufstiegserlaubnis zugeordnet und damit der Betreiber sowie die Details des Drohneneinsatzes ermittelt werden können. Die Aufgaben der Luftfahrtbehörde sind im Land Sachsen-Anhalt dem Landesverwaltungsamt (Referat Verkehrswesen) zugeordnet. Bei erlaubnisfreiem Einsatz der Drohnen könnte eine Anfrage bei der örtlichen Polizei- oder Ordnungsbehörde oder beim Landesbeauftragten zielführend sein, wenn der Betreiber dort aufgrund eines häufigeren Einsatzes bekannt ist. Es wird jedoch vermutlich auch Fälle geben, in denen der Landesbeauftragte mangels Kenntnis des Betreibers die Einhaltung des Datenschutzes nicht kontrollieren kann.

15.2.13 Wildkameras

In seinem XI. Tätigkeitsbericht (Nr. 4.17.6) hat der Landesbeauftragte bereits den Rechtsrahmen beschrieben, in dem die Benutzung von Wildkameras in Wald und Feld möglich wäre. Es wurde dargelegt, dass Wald i. d. R. nach dem FFOG öffentlich zugänglichen Raum darstellt. Die Videoüberwachung unterliegt also in solchen Fällen den Vorgaben des § 6b BDSG. Durch unterschiedliche Regelungen ist allerdings vorgegeben, dass einzelne Bereiche des Waldes nicht für jedermann betretbar sind, also keinen öffentlichen Raum i. S. d. § 6b BDSG darstellen. Im Berichtszeitraum wurde der Landesbeauftragte befragt, wie Wildkameras zu bewerten sind, die diese Waldbereiche ablichten.

Spezialgesetzliche Betretungseinschränkungen finden sich neben dem Naturschutzrecht (vgl. XI. Tätigkeitsbericht, Nr. 4.17.6) z. B. auch im FFOG bzw. im LJagdG. So dürfen ohne Einwilligung des Nutzungsberechtigten, also z. B. des Jagdausübungsberechtigten, nach § 3 Abs. 2 Nr. 1 f) FFOG u. a. jagdwirtschaftliche Einrichtungen nicht betreten werden. Obgleich Kirrungen, also Plätze, an die jagdbares Wild mit Futter gelockt wird, in der Liste der jagdwirtschaftlichen Einrichtungen in § 3 Abs. 2 Satz 1 LJagdG nicht enthalten sind, werden solche Plätze doch überwiegend als solche Einrichtungen angesehen, z. B. in einem Urteil des Landgerichts Essen vom 26. Juni 2014 (Az. 10 S 37/14). Das Landgericht kommt zu der Feststellung, dass der die Videoüberwachung im öffentlichen Raum regelnde § 6b BDSG nicht zur Anwendung kommt, wenn jagdrechtliche Betretungsverbote bestehen, was auch für Kirrungen gilt.

Allerdings wären in diesen Fällen die Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG zu prüfen. Daraus folgt, dass auch in betretungsbeschränkten Bereichen von Wald und Feld datenschutzrechtliche Vorgaben einzuhalten sind. Dies ist auch notwendig, da sich hier bestimmte Personen berechtigterweise aufhalten können, z. B. der Grundeigentümer, der seinen Grund an Jäger verpachtet hat, oder Feld- und Waldarbeiter. Deren schutzwürdige Interessen müssen hier angemessen berücksichtigt werden. Voraussetzung für die Anwendung des § 28 Abs. 1 Nr. 2 BDSG ist jedoch, dass diese Bereiche erkennbar sind (Landgericht Essen, a. a. O). Hier besteht das Problem, dass Kirrungen als betretungsbeschränkte jagdliche Einrichtungen von öf-

fentlich zugänglichem Raum umschlossen werden, ohne von diesem immer sichtbar abgegrenzt zu sein. Die Jagdausübungsberechtigten hätten aber die Möglichkeit, durch geeignete Beschilderung die Kirrungen als betretungsbeschränkte jagdliche Einrichtung zu kennzeichnen. So würde wohl auch unwahrscheinlicher, dass ahnungslose Waldbesucher ausgerechnet in der Nähe der Kirrung Pilze suchen. Soweit es trotz der erkennbaren Betretungsbeschränkung zur Erhebung personenbezogener Daten kommt, würden i. d. R. die berechtigten Interessen des Jagdausübungsberechtigten gegenüber den Interessen der aufgenommenen Personen überwiegen. Nicht erkennbare Kirrungsplätze sind nach Ansicht des Landesbeauftragten rechtlich wie öffentlich zugänglicher Raum zu behandeln. Eine Videoüberwachung mittels Wildkamera wäre demnach auch dort nur unter Heranziehung des § 6b Abs. 2 BDSG zulässig, nach dem der Umstand der Videoüberwachung und die verantwortliche Stelle vorgelagert geeignet erkennbar zu machen sind.

16 Verkehr

16.1 Die Pkw-Maut – Infrastrukturabgabe auf Bundesfernstraßen

Bereits mit dem Bekanntwerden der Pläne des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) Anfang des Jahres 2014 zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen, in den öffentlichen Medien auch als „Pkw-Maut“ bezeichnet, begegnete dieses Vorhaben grundsätzlichen datenschutzrechtlichen Bedenken.

Mit dieser Ausweitung der Nutzerfinanzierung auf Pkw und Wohnmobile mit bis 3,5 t Gesamtgewicht sollen die dringend erforderlichen Verkehrsinfrastrukturinvestitionen für die Erhaltung und den weiteren Ausbau des Bundesfernstraßennetzes realisiert werden. Für Halter von im Inland und im Ausland zugelassenen Pkw und Wohnmobilen soll eine Infrastrukturabgabe für die Nutzung von Bundesautobahnen und Bundesstraßen eingeführt werden. Halter von nicht in Deutschland zugelassenen Pkw und Wohnmobilen sind nur bei der Nutzung von Bundesautobahnen abgabenpflichtig. Kraftfahrzeuge u. a. von Personen mit Behinderungen, die ganz oder teilweise von der Kfz-Steuer befreit sind, werden der Infrastrukturabgabe nicht unterworfen.

Wo liegen nun die grundsätzlichen datenschutzrechtlichen Probleme des mit Art. 1 des Gesetzes zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen vom 8. Juni 2015 beschlossenen Gesetzes über die Erhebung einer zeitbezogenen Infrastrukturabgabe für die Benutzung von Bundesfernstraßen (Infrastrukturabgabengesetz – InfrAG) (BGBl. I S. 904), welches am 12. Juni 2015 in Kraft getreten ist.

Grundsätzlich stellt sich die Frage, warum noch eine Kontrolle der „elektronischen Vignette“ durch Kennzeichen-Scanning erfolgen muss, wenn zukünftig in Deutschland ein Kraftfahrzeug nur zugelassen werden kann, wenn der Fahrzeughalter wie beim Einzug der Kfz-Steuer auch für die sogenannte Infrastrukturabgabe gemäß § 5 Abs. 2 InfrAG ebenfalls die Ermächtigung zum Einzug beim Kraftfahrt-Bundesamt (KBA) durch ein SEPA-Lastschrift-Mandat erteilen muss und eine Zulassung gemäß § 9 Abs. 3 InfrAG bei Nichterteilung eines SEPA-Lastschrift-Mandat zu versagen ist. Die nach Landesrecht zuständige Zulassungsbehörde kann sogar gemäß § 9 Abs. 6 InfrAG bei Nichtentrichtung der Infrastrukturabgabe auf Antrag des KBA eine Abmel-

dung des Kraftfahrzeuges von Amt wegen vornehmen und das Kraftfahrzeug außer Betrieb setzen. Eine solche elektronische Kontrolle ist aus datenschutzrechtlicher Sicht daher weder verhältnismäßig noch erforderlich. Diese Kontrolle könnte auch stichprobenartig bei der Überprüfung von Kraftfahrzeugen durch das Bundesamt für Güterverkehr (BAG) oder die Polizeibehörden durchgeführt werden.

Mit diesem Gesetz wird jedoch eine neue Kontrollinfrastruktur geschaffen. Gemäß § 4 InfrAG ist das Kraftfahrt-Bundesamt (KBA) als Infrastrukturbehörde für die Erhebung und zentrale Speicherung der Daten in einem Infrastrukturabgaberegister (§ 6 InfrAG) sowie für die Erstellung der Bescheide zuständig. Das KBA kann zudem gemäß § 4 Abs. 1 Satz 2 InfrAG privaten Dritten (sog. „Betreiber“) die Erhebung der Infrastrukturabgabe, die Durchführung der Mahnungen nach dem Verwaltungsvollstreckungsgesetz und den Erlass von Vollstreckungsanordnungen übertragen.

Die Überwachung der Einhaltung der Abgabepflicht erfolgt gemäß § 11 Abs. 1 Satz 1 InfrAG durch das BAG, welches sich dabei gemäß § 11 Abs. 1 Satz 2 InfrAG ebenfalls der Mitwirkung privater Dritter bedienen kann. Zum Zwecke der Überwachung können das BAG und die beauftragten Dritten gemäß § 11 Abs. 2 InfrAG im Rahmen einer Vor-Ort-Kontrolle u. a. auch das Bild des Kraftfahrzeuges (ohne Insassen), Name und Anschrift des Kraftfahrzeugführers, Ort und Zeit der Benutzung von Straßen sowie das amtliche Kennzeichen erheben, speichern und nutzen. Auch wenn diese Daten ausschließlich zum Zweck der Überwachung der Einhaltung der Vorschriften des InfrAG verarbeitet und genutzt werden dürfen, besteht die nicht unberechtigte Sorge, dass auch, wie bereits bei der Lkw-Maut in der Vergangenheit, Begehrlichkeiten zur weiteren „Nutzung“ dieser Daten durch die Sicherheitsbehörden entstehen könnten, denn Gründe lassen sich immer finden.

Mit dieser zentralen Speicherung, der Überwachung und der umfangreichen Datenübermittlung zwischen KBA, BAG und den beauftragten privaten Dritten werden zumindest die Voraussetzungen und Möglichkeiten der Erstellung umfangreicher Bewegungsprofile aller Kraftfahrzeugbenutzer auf Bundesfernstraßen geschaffen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat nach Bekanntwerden des Gesetzentwurfes des BMVI bereits frühzeitig am 14. November 2014 mit der Entschließung „Keine Pkw-Maut auf Kosten des Datenschutzes“ (**Anlage 19**) die Schaffung eines zentralen Infrastrukturabgaberegisters, die Einbeziehung privater Dritter bei Erhebung und Überwachung der Infrastrukturabgabe sowie die damit verbundenen Befugnisse der Datenerhebung und -verarbeitung abgelehnt und die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlichen Prinzipien der Datenvermeidung und Datensparsamkeit ermahnt. Diesen datenschutzrechtlichen Bedenken wurde, auch wenn es hinsichtlich der Speicher- und Löschfristen sowie der Zweckbindung dieser Daten Verbesserungen im in Kraft getretenen InfrAG gibt, nicht in vollem Umfang Rechnung getragen.

Nach dem Vorbild anderer europäischer Staaten gibt es zudem mildere und effektivere Mittel und Möglichkeiten (z. B. Papiervignette) zur Kontrolle der Entrichtung der Infrastrukturabgabe. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Kraftfahrzeuge bzw. für die Nichtnutzung des Bundesfernstraßennetzes erstatten zu lassen, rechtfertigt nicht die elektronische Überwachung und Speicherung in diesem Umfang und mit diesem Aufwand.

Nur um nachträglich einen Erstattungsanspruch prüfen zu können, werden an allen Orten und Zeiten, zu denen ein Kraftfahrzeug eine mautpflichtige Bundesfernstraße benutzen würde, umfangreich personenbezogene Daten gespeichert. Mit diesen könnten vollständige Bewegungsprofile erstellt werden, sollte die Infrastrukturabgabe in dieser Form eingeführt werden. Diese Art der Vorratsdatenspeicherung ist weder verhältnismäßig noch erforderlich. Ausreichend wäre eine einfache gesetzliche Regelung über eine zeitanteilige Erstattung der Infrastrukturabgabe, wenn ein Kraftfahrzeug abgemeldet bzw. das Fahrzeug nachweislich das ganze Jahr über nicht auf mautpflichtigen Straßen bewegt worden wäre.

Der Landesbeauftragte hatte auch das Ministerium für Landesentwicklung und Verkehr (MLV) von dieser Entschließung in Kenntnis gesetzt. Das MLV hatte im Dezember 2014 in seiner Stellungnahme zum damaligen Gesetzentwurf (Stand: 9. Dezember 2014) das BMVI knapp gebeten, besonderes Augenmerk auf die datenschutzrechtlichen Aspekte zu legen. Da wäre aber mehr Unterstützung zu erwarten gewesen.

Inwieweit diese geplante Pkw-Maut die europarechtlichen Vorgaben der Nicht-Diskriminierung von Ausländern erfüllt, ist allerdings mehr als fraglich. Die EU-Kommission eröffnete nach dem In-Kraft-Treten des InfrAG und des Zweiten Gesetzes zur Änderung des Kraftfahrzeugsteuergesetzes (KraftStG) vom 8. Juni 2015 (BGBl. I S. 901) ein Vertragsverletzungsverfahren gegen dieses Vorhaben der Bundesregierung. Im geänderten KraftStG wurde eine Steuerermäßigung durch Berücksichtigung eines Entlastungsbetrages aufgenommen, die es vermeiden soll, dass inländische Steuerpflichtige durch die Einführung der Infrastrukturabgabe doppelt belastet werden.

Der Bundesverkehrsminister reagierte darauf mit einer Verschiebung der Einführung der Infrastrukturabgabe, die eigentlich zu Beginn des Jahres 2016 erfolgen sollte. Falls es zu keiner Einigung der Bundesregierung mit der EU-Kommission kommen sollte, könnte sich der Einführungstermin bis zu einer möglichen Entscheidung durch den Europäischen Gerichtshof damit um Jahre verschieben. Ein Gutachten des Fachbereichs Europa der Wissenschaftlichen Dienste des Bundestages vom 9. Juli 2015 (Az. PE 6 - 3000 - 68/15) untermauert die Einschätzung der EU-Kommission, wonach gerade die Kombination der beiden zeitgleich verabschiedeten Gesetze eine „mittelbare Diskriminierung aus Gründen der Staatsangehörigkeit“ darstellen könnte.

Das Thema Pkw-Maut wird die Datenschutzbeauftragten und auch die Öffentlichkeit deshalb noch längere Zeit beschäftigen. Eine Papiervignette wäre die datenschutzgerechte Lösung, denn für diese Form der Mauterhebung, die bereits in vielen europäischen Staaten seit langem so praktiziert wird, brauchen keine personenbezogenen Daten der Mautpflichtigen erhoben zu werden.

16.2 VEMAGS-Staatsvertrag – Entwurf mit Mängeln

Die Bearbeitung von StVO-Anträgen zur Durchführung von Großraum- und Schwertransporten erfolgt bundesweit in einem automatisierten Verfahren unter der Bezeichnung VEMAGS (Verfahrensmanagement für Großraum- und Schwertransporte). Grundlage für die Entwicklung und den vorläufigen Betrieb von VEMAGS ist bisher eine zwischen den Ländern abgeschlossene Verwaltungsvereinbarung, die als Rechtsgrundlage nicht ausreichend ist, auch wenn gemäß Art. 91c Abs. 3 GG die

Länder den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren können. Seit 2008 wird das Verfahren flächendeckend in allen Ländern genutzt und steht damit den Antragstellern von Groß- und Schwerlasttransporten bundesweit zur Verfügung. Mit der Überführung des Testbetriebs in den ständigen Regelbetrieb im Jahr 2012 besteht seitens der Datenschutzbeauftragten des Bundes und der Länder die nachdrückliche Forderung nach einer gesetzlichen Grundlage.

Der Landesbeauftragte hatte in seinem XI. Tätigkeitsbericht (Nr. 13.6.1) das VEMAGS-Verfahrens-Modul vorgestellt und über den damaligen Sachstand berichtet. In der Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht (LT-Drs. 6/3512 vom 15. Oktober 2014) wurde auf dieses Thema nicht eingegangen. Eine weitere unmittelbare Beteiligung und Information zum Verfahrensstand vom zuständigen Ministerium für Landesentwicklung und Verkehr (MLV) erfolgte allerdings nicht. Erst durch die Information eines anderen Landesbeauftragten, der seitens des zuständigen Ministeriums um Stellungnahme zu einem Entwurf eines Staatsvertrags (Stand: 11. Juni 2014) aufgefordert wurde, erhielt der Landesbeauftragte davon Kenntnis. Im Januar 2015 übersandte der hessische Landesbeauftragte im Auftrag des Hessischen Verkehrsministeriums einen fortgeschriebenen Entwurf dieses Staatsvertrages (Stand: 15. Dezember 2014).

Eine Nachfrage beim MLV hinsichtlich der weiteren Verfahrensweise ergab, dass das Thema VEMAGS Gegenstand der Gemeinsamen Konferenz der Verkehrs- und Straßenbauabteilungsleiter (GKVS) im März 2015 war, derzeit aber nicht absehbar wäre, wann ein Staatsvertrag abgeschlossen werden könnte. Das Land Hessen wurde laut Beschluss der GKVS gebeten, die Entwicklung des Projektes weiter zu begleiten.

Grundsätzlich ist es begrüßenswert, dass das Verfahren VEMAGS mit einem Staatsvertrag endlich auf eine rechtliche Grundlage gestellt werden soll. Allerdings muss auch für den fortgeschriebenen Entwurf des Staatsvertrags festgestellt werden, dass noch wesentliche datenschutzrechtliche Mängel bestehen. Das betrifft insbesondere die Regelungen in Art. 3 (Verantwortlichkeit für die Einrichtung und den Betrieb des Systems VEMAGS) und Art. 5 (Datenschutz) des Entwurfs.

Eine Hauptforderung des Datenschutzes – die Vermeidung einer wechselnden verantwortlichen Stelle – wurde leider auch im nunmehr vorliegenden Entwurf nicht berücksichtigt. Gemäß Art. 3 Abs. 2 des Entwurfs soll die Projektleitung VEMAGS, die zugleich die nach Art. 5 Abs. 2 des Entwurfs datenschutzrechtlich verantwortliche Stelle sein soll, jeweils nur befristet einem Vertragspartner übertragen werden. Dieses Rotationsprinzip der verantwortlichen Stelle ist datenschutzrechtlich bedenklich und kaum praktikabel, denn das anzuwendende Datenschutzregime soll sich gemäß Art. 5 Abs. 11 des Entwurfs nach dem Sitzlandprinzip, d. h. nach dem Sitz der Projektleitung VEMAGS und dem für sie geltenden Landesdatenschutzgesetz, richten.

Die geplante Regelung in Art. 5 Abs. 10 des Entwurfs zu den technischen und organisatorischen Maßnahmen, die über ein Sicherheitskonzept sichergestellt werden sollen, welches zumindest mit dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik konform sein soll, ist zwar zu begrüßen, berücksichtigt aber nicht im vollem Umfang datenschutzrechtliche Ziele der Datensicherheit der jeweiligen Landesdatenschutzgesetze. Zumindest bedarf es einer Klarstellung im Staatsvertrag, dass weitere Anforderungen an technische und organisatorische

Maßnahmen nach dem für die verantwortliche Stelle allgemein geltenden Datenschutzrecht unberührt bleiben, für Sachsen-Anhalt wären es u. a. die §§ 6, 7, 7a und 8 DSG LSA.

Der Landesbeauftragte fordert deshalb das MLV auf, sich aktiv für die Umsetzung der datenschutzrechtlichen Forderungen bei der weiteren Überarbeitung des Entwurfs einzusetzen und ihn rechtzeitig zu beteiligen.

16.3 Der gläserne Autofahrer – Datenschutz im Kraftfahrzeug

Moderne Kraftfahrzeuge sind nicht nur ein Fortbewegungsmittel, sie haben sich mittlerweile auch zu wahren „Datensammlern“ entwickelt. Eine Vielzahl von verschiedenen Geräten und Systemen überwachen und speichern schon heute alles das, was sich in und an einem modernen Kraftfahrzeug ereignet. Damit ist wiederum die Möglichkeit gegeben, aufschlussreiche Kenntnis über Fahrstrecken und Fahrverhalten der Autofahrer zu erlangen.

Das Internet hält nicht nur Einzug in Smartphones und Tablets, sondern wird zunehmend in modernen Kraftfahrzeugen integriert. Internetkonzerne wie Google und Apple treiben die Entwicklung des autonom fahrenden Automobils voran, und auch führende deutsche Automobilkonzerne statten ihre Kraftfahrzeuge mit modernen Assistenz- und Kommunikationssystemen aus, mit dem Ziel der Vernetzung der Fahrzeuge mit dem Internet, untereinander oder mit der Verkehrsinfrastruktur auf der Straße.

Die Europäische Union (EU) verfolgt dieses Ziel der Schaffung intelligenter Verkehrssysteme mit autonom und vernetzt agierenden Kraftfahrzeugen bereits seit dem Jahr 2006 und hat daraus ein Regelwerk für intelligente Verkehrssysteme entwickelt, das zugleich zu mehr Verkehrssicherheit beitragen soll. Ein Ergebnis dieser Initiativen auf europäischer Ebene war die am 7. Juli 2010 erlassene Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 S. 1). Im Jahr 2013 wurde sie durch das Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG) vom 11. Juni 2013 (BGBl. I S. 1553) in nationales Recht umgesetzt. Ziel der Richtlinie ist es, dass sich „Intelligente Verkehrssysteme“ der Mitgliedstaaten der EU an den in der Richtlinie aufgeführten Spezifikationen ausrichteten, damit die Systeme innerhalb Europas kompatibel sind. Das IVSG sieht in § 5 eine Ermächtigung für das damalige Bundesministerium für Verkehr, Bau und Stadtentwicklung vor, durch Rechtsverordnung mit Zustimmung des Bundesrats die Anforderungen an intelligente Verkehrssysteme in vorrangigen Bereichen (§ 4 IVSG) zu regeln. Bisher wurde durch das nunmehr zuständige Bundesministerium für Verkehr und digitale Infrastruktur von dieser Verordnungsermächtigung noch kein Gebrauch gemacht. Der Datenschutz könnte dabei ins Hintertreffen geraten, wenn die rechtlichen Rahmenbedingungen nicht rechtzeitig geklärt werden, denn auch in diesen intelligenten Verkehrssystemen können eine Vielzahl personenbezogener Daten erhoben und verarbeitet werden.

Als eines der ersten „Intelligenten Systeme“ soll nach dem Willen der EU der automatische Notruf „eCall“ eingeführt werden. Das System soll im Falle eines Autounfalls automatisch und über das Mobilfunknetz die örtlich zuständige eCall-Notrufabfragestelle informieren, wobei die Positionsdaten des Unfallautos übertragen und eine Sprechverbindung zwischen dem Fahrzeug und der eCall-

Notrufabfragestelle aufgebaut werden soll. Mit delegierter Verordnung (EU) Nr. 305/2013 vom 26. November 2012 (ABl. 2013 L 91 S. 1) hat die Kommission die Spezifikationen für die Infrastruktur der eCall-Notrufabfragestellen festgelegt, die bis zum 1. Oktober 2015 einzurichten sind. Am 13. Juni 2013 hat die Europäische Kommission außerdem ihren Vorschlag für eine EU-Verordnung über die Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeugen vorgestellt (COM(2013) 315 final).

Schon heute verfügen moderne Kraftfahrzeuge vielfach über Assistenzsysteme, die den Autofahrer unter Zuhilfenahme von Informations- und Kommunikationstechnologien unterstützen wie z. B. Antiblockiersysteme, Bremsassistenten, Kollisionswarnsysteme, Spurhaltesysteme, Geschwindigkeits- und Abstandsregelungssysteme oder automatische Einparkhilfen.

Die Forschungs- und Entwicklungsarbeiten gehen aber bereits viel weiter. Zwei in Zusammenhang stehende Entwicklungstendenzen sind erkennbar:

Zum einen sollen die Assistenzsysteme weiter so ausgebaut werden, dass sich das Kraftfahrzeug der Zukunft *autonom*, ohne Steuerung durch den Menschen, sicher im Straßenverkehr fortbewegen kann. Zum anderen steht das *vernetzte* Kraftfahrzeug im Fokus der Forschung und Entwicklung. Es soll in Zukunft mehr und mehr Kontakt mit seiner Umwelt, d. h. mit anderen Kraftfahrzeugen, aber auch mit der Verkehrsinfrastruktur aufnehmen und *kommunizieren*. Schlagworte hierzu lauten „Connected Car“, „Car-to-Car“, „Car-to-X“. Als „Connected Car“ werden demnach Kraftfahrzeuge bezeichnet, die über einen Internetzugang sowie über weitere Kommunikationsschnittstellen wie z. B. WLAN und Bluetooth verfügen und sich dabei die Internetverbindung mit anderen Geräten teilen. Autofahrer sollen so mittels der kommunizierenden Kraftfahrzeuge auf diese Weise z. B. frühzeitig über die auf ihrer Route befindlichen Straßenzustände, Baustellen, Staus, Unfälle, und andere Verkehrssituationen informiert werden. Das Autofahren soll durch autonom gesteuerte und kommunizierende Kraftfahrzeuge angenehmer, stressfreier, sicherer und flüssiger werden.

Schon seit 2009 arbeiten große europäische Automobilhersteller wie u. a. die Volkswagen AG erfolgreich mit Google an der Integration von sog. Mehrwertdiensten in das Kraftfahrzeug. Anfang des Jahres 2014 hat z. B. der Internetkonzern Google zusammen mit führenden Automobilherstellern und namhaften Unternehmen der IT-Branche die Open Automotive Alliance (OAA) ins Leben gerufen. Ziel der OAA ist es, das von Google entwickelte Betriebssystem Android in das Kraftfahrzeug zu integrieren und damit den Nutzungsbedürfnissen von Autofahrern anzupassen. Die OAA legt die Schnittstelle „Android Auto“ als Standard für die Integration von Android-Geräten fest. Android Auto ist der nächste Schritt im Bereich Konnektivität und verknüpft Smartphones bzw. Tablets mit dem Infotainment-System moderner Kraftfahrzeuge. Per Android Auto verbinden sich Android-Smartphones mit dem Infotainment-System des Autos, welches lediglich als Bildschirm und Eingabegerät dient. Anwendungen laufen komplett auf dem Smartphone, das das Bild weitergibt und auf Eingaben über den Touchscreen des Infotainment-Systems des Kraftfahrzeuges oder auch über Sprachbefehle reagiert. Medienberichten zufolge wollten 35 führende Automobilkonzerne, darunter auch europäische Automarken, noch im Jahr 2015 Android Auto in ihre Neufahrzeuge bringen. Eine ähnliche Zielstellung verfolgt der Internetkonzern Apple bereits seit 2014 mit seinem System unter dem Namen

„CarPlay“, das die Verbindung zwischen dem iPhone und dem Infotainment-System im Kraftfahrzeug ermöglicht.

Hieraus ergeben sich eine ganze Reihe von datenschutzrechtlichen Problemen und Fragestellungen: Wie gläsern ist der Autofahrer in seinem Auto? Welcher gesetzliche Regelungsbedarf besteht? Und nicht zuletzt die Frage: Wem gehören die Daten, die beim Betrieb des Kraftfahrzeugs und seiner Kommunikation mit der Außenwelt entstehen und wer darf darauf zugreifen?

Zu Beginn des Jahres 2014 hatte sich der 52. Verkehrsgerichtstag in Goslar dem Thema Datenschutz im Kraftfahrzeug gewidmet unter der Fragestellung „Wem gehören die Fahrzeugdaten?“. Diese bereits in der Vergangenheit oft gestellte Frage, wem die Daten „*gehör*en“, ist etwas irreführend, da das Datenschutzrecht nicht auf dem „Eigentum“ an Daten basiert, sondern die datenschutzrechtlichen Fragen nach der Betroffenheit und der verantwortlichen Stelle beantwortet werden müssen. Dieses Thema hat die Datenschutzbeauftragten des Bundes und der Länder im zurückliegenden Berichtszeitraum beschäftigt und zu einem Dialog mit der Automobilindustrie, vornehmlich dem Verband der deutschen Automobilindustrie (VDA), der Hersteller wie Zulieferer vertritt, geführt. Hierzu begannen Ende des Jahres 2014 direkte Gespräche zwischen Vertretern des Arbeitskreises Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und dem VDA.

Folgende Themenfelder standen dabei im Fokus und bedürfen einer weiteren intensiven Erörterung, Diskussion und Beurteilung sowohl mit den Automobilherstellern als auch mit der Politik:

Thema: Fahrzeugdatenspeicher

Hierbei geht es um Daten, die in den Speichermedien der elektronischen Steuerungseinheiten gesammelt werden (Betriebsdaten), z. B. Geschwindigkeit, Bremsbetätigung, Beschleunigung, Füllstande und viele weitere mehr, die dazu dienen, eine störungsfreie Nutzung des Kraftfahrzeuges zu ermöglichen und für etwaige Wartungs-, Diagnose- oder Reparaturarbeiten zur Verfügung zu stehen. Grundsätzlich stellt sich hier die Frage, ob diese „nur“ technischen Daten in gewissen Verwendungszusammenhängen nicht doch eine Datenschutzrelevanz besitzen.

Thema: Europäischer Notruf (eCall)

Die EU führt ein europaweites Notrufsystem eCall verbindlich ein. Spätestens ab April 2018 wird das Notrufsystem eCall für alle Neufahrzeuge zur Pflicht und soll bei schweren Autounfällen automatisch per Mobilfunkverbindung über die europaweite Notrufnummer 112 die Rettungsdienste benachrichtigen und eine Kommunikation zum Autofahrer aufbauen. Die Rettungsdienste erhalten auf diesem Weg in einem Minimaldatensatz Angaben zum Standort, zur Fahrtrichtung, zum Unfallzeitpunkt, zur Anzahl der Insassen und zum Fahrzeugtyp, um so schnell und effizient Hilfe zu leisten. Der eCall-Notruf kann auch vom Autofahrer manuell ausgelöst werden. Er ist im Normalfall abgeschaltet und wird erst bei einem Unfall – automatisch oder manuell – aktiviert. Die Datenverarbeitung für den eCall ist auf die Rettungsleitstelle und ihre Hilfsmaßnahmen beschränkt. Eine Ortung findet nur im Notfall statt.

Thema: Mehrwertdienste

Während gegen den auf Notfälle und Rettungsmaßnahmen bezogenen eCall datenschutzrechtlich grundsätzlich keine Bedenken erhoben werden, ist der parallele Einsatz dieser kommerziellen Mehrwertdienste datenschutzrechtlich kritischer zu betrachten. Beispiele für Mehrwertdienste sind besondere Dienstleistungsangebote der Automobilhersteller mit auf die Automarke zugeschnittenem Pannenruf, Dienste der Versicherungen bei Unfällen und Beschädigungen, sowie weitere internetbasierte Serviceangebote. Der Markt der Mehrwertdienste wird von den Automobilherstellern und ihren Vertragswerkstätten, von den Versicherern, den Mobilfunkanbietern und den Automobilclubs sowie von zahlreichen anderen Internetfirmen stark umworben, denn diese Dienste sind in der Regel kostenpflichtig und benötigen eine permanente Mobilfunkanbindung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fasste am 8. und 9. Oktober 2014 die Entschließung „Datenschutz im Kraftfahrzeug – die Automobilindustrie ist gefordert“ (**Anlage 16**). Danach sind Automobilhersteller, Händler, Werkstätten sowie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihrer Verantwortung in der Pflicht, das informationelle Selbstbestimmungsrecht im und um das Kraftfahrzeug zu gewährleisten. Wesentliche Forderungen sind:

- Die Berücksichtigung der Datenschutzgrundsätze von Privacy by Design und Privacy by Default bereits in der Konzeptionsphase der Entwicklung neuer Fahrzeugmodelle und der darauf zugeschnittenen Angebote für Kommunikations- und Teledienste (Mehrwertdienste)
- Die Umsetzung des Prinzips der Datenvermeidung und Datensparsamkeit bei Datenverarbeitungsvorgängen im und um das Fahrzeug sowie einer möglichst zeitnahen Löschung nicht mehr benötigter Daten
- Die Datenverarbeitung entweder auf vertraglicher Vereinbarung oder auf eine informierte Einwilligung des Fahrzeughalters zu stützen
- Die Gewährleistung der vollständigen Transparenz für Fahrzeughalter bzw. Fahrzeugführer durch umfassende, verständliche und schriftliche Information, welche Daten beim Betrieb des Kraftfahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden
- Die Erkennbarkeit, Kontrolle sowie ggf. Löschungs- und Unterbindungsmöglichkeit von Datenübermittlungen rechtlich wie technisch auch bei einer vertraglich vereinbarten oder durch Einwilligung getragenen Datenübermittlung an Automobilhersteller oder sonstige Diensteanbieter für den Fahrzeughalter bzw. Fahrzeugführer
- Die Sicherstellung und Gewährleistung der Datenintegrität und der Datensicherheit durch geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik, insbesondere auch für die Datenkommunikation aus dem Kraftfahrzeug heraus

Die kurze Zeit später im November 2014 vom VDA veröffentlichten „Datenschutz-Prinzipien für vernetzte Fahrzeuge“ beinhalten zwar solche Grundsätze wie Transparenz, Selbstbestimmung und Datensicherheit und sind damit zumindest ein erster Schritt auf den Weg zu einem verlässlichen Datenschutz, lassen aber noch viele

Fragestellungen offen. Das betrifft insbesondere die Interpretation der Datenschutzrelevanz zu einzelnen Datenkategorien, wie z. B. der im Kraftfahrzeug erzeugten „technischen Daten“, durch den VDA. Diese können durchaus in anderen Verwendungszusammenhängen und Kombinationen datenschutzrelevant werden. Zudem beschränkt der VDA diese Datenschutzprinzipien auf das vernetzte Kraftfahrzeug und trifft keine Aussagen zu den im Kraftfahrzeug vorhandenen Fahrzeugdatenspeichern und deren Zugriffsmöglichkeiten durch Dritte. Die Gespräche mit dem VDA wurden im Jahr 2015 in einer konstruktiven Atmosphäre fortgesetzt. Im Ergebnis wurde eine gemeinsame Erklärung von VDA und Datenschutzkonferenz zu den vorerwähnten Aspekten gefasst[14].

16.4 Runderlass zum ruhenden Verkehr

In seinem XI. Tätigkeitsbericht (Nr. 13.6.4) hatte der Landesbeauftragte auf die datenschutzrechtlich unzulässige Speicherung von Verwarnungen auf Vorrat im ruhenden Verkehr im Rahmen eines Modellversuches einer Stadt hingewiesen. Zwischenzeitlich hat das Ministerium für Inneres und Sport den Modellversuch rechtlich beurteilt und die Auffassung des Landesbeauftragten zur datenschutzrechtlichen Unzulässigkeit dieser Vorratsdatenspeicherung bestätigt. Danach hat das Landesverwaltungsamt über die Kommunalaufsicht des Landkreises die Stadt im August 2013 aufgefordert, diesen Modellversuch einzustellen und die bisher erhobenen und gespeicherten Daten zu löschen.

Die betreffende Stadtverwaltung zeigte sich erst spät einsichtig und musst nochmals aufgefordert werden, die Beendigung des Modellversuches und die Löschung der Daten gegenüber dem Landesbeauftragten zu bestätigen. Diese Bestätigung erfolgte dann endlich im Januar 2014.

Die Landesregierung hatte als Reaktion auf den Beitrag im XI. Tätigkeitsbericht in ihrer Stellungnahme vom 15. Oktober 2014 (LT-Drs. 6/3512) die Prüfung eines Erlasses in Aussicht gestellt, der auf die geltende Rechtslage und die Unzulässigkeit solcher Vorratsdatenspeicherung hinweisen sollte.

Bereits im Januar 2015 wurde der Landesbeauftragte gemäß § 14 Abs. 1 Satz 3 DSG LSA durch das Innenministerium zur Stellungnahme zum Erlassentwurf gebeten. Das Ministerium folgte dabei auch der Empfehlung des Landesbeauftragten, den Erlass nicht nur an das Landesverwaltungsamt zu richten, sondern als Runderlass im Ministerialblatt des Landes zu veröffentlichen. Nur so konnte nach Meinung des Landesbeauftragten eine Information an alle Städte und Gemeinden und nicht zuletzt auch für die Bürgerinnen und Bürger sichergestellt werden. Die Veröffentlichung des Runderlasses vom 6. März 2015 erfolgte dann am 30. März 2015 (MBl. LSA S. 162).

[14] http://lsaurl.de/DSimKfzErkl

Anlagen

Nationale Datenschutzkonferenz

Anlage 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u.a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.

- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

  Dazu gehört,

  - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.

  - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.

  - die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.

- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.

- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

Anlage 2

Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 in Bremen

Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ (Anlage 1) verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Da-

tenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

Anlage 3

Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 in Bremen

Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt – wie repräsentative Studien belegen – mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.[1]

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.[2]

- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und

[1] Siehe dazu die Entschließungen „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ (Anlage 1) und „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“ (Anlage 2).

[2] Siehe dazu die heutige Entschließung „Stärkung des Datenschutzes im Sozial- und Gesundheitswesen“ (Anlage 4).

die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.[3]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

[3] Siehe dazu die heutige Entschließung „Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“ (Anlage 5).

Anlage 4

Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 in Bremen

Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von „gläsernen Patientinnen und Patienten oder Versicherten“ weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen

und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

Anlage 5

Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013 in Bremen

Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung „Sicherheit bei E Government durch Nutzung des Standards OSCI“ Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, sodass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

Anlage 6

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,

2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,

6. Ausbau der Angebote und Förderung anonymer Kommunikation,

7. Angebot für eine Kommunikation über kontrollierte Routen,

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,

9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,

11. Sensibilisierung von Nutzern moderner Technik,

12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage 7

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Anlage zur Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

1. *Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten*

   Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographischen Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. *Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungsinfrastruktur*

   Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises. Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung*

   Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den

Endpunkten erreicht werden. Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. *Sichere und vertrauenswürdige Bereitstellung von Internetangeboten*

   Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. *Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten*

   Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. *Ausbau der Angebote und Förderung anonymer Kommunikation*

   Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzern müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. *Angebot für eine Kommunikation über kontrollierte Routen*

   Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird.

   Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder

Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. *Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung*

   Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzer genutzt werden können. Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

   - alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,

   - für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,

   - eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und

   - die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

   Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken. Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen.

   Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. *Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik*

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist. Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. *Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung*

    Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern. Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. *Sensibilisierung von Nutzern moderner Technik*

    Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. *Ausreichende Finanzierung für Maßnahmen der Informationssicherheit*

    Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

Anlage 8

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzer der Sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- Es ist sicherzustellen, dass

    - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

    - die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,

    - die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Anlage 9

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Anlage 10

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, sodass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm PRISM, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4a BDSG rechtmäßig erfolgen.

- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionswei-

se der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.

- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Anlage 11

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

- Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

- Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Orte der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

- Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

- Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall

zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

- Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

- Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

- Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

Anlage 12

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. April 2014

Ende der Vorratsdatenspeicherung in Europa!

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z. B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

Anlage 13

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle

Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anlage 14

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg

Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Anlage 15

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Anlage 16

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fah-

rer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anlage 17

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg

Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BR-Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes- und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetzes nicht der Fall.

- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentschei-

dungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Anlage 18

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage 19

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Keine PKW-Maut auf Kosten des Datenschutzes!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 20

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

Anlage 21

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. Februar 2015

Keine Cookies ohne Einwilligung der Internetnutzer

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann z. B. auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Art. 5 Abs. 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sog. Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Anlage 22

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

Anlage 23

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (“Predictive Policing“).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauf-

tragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

Anlage 24

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Anlage 25

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Anlage 26

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Straf-

verfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

Anlage 27

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,

- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und

- kryptographische Technologien in E Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

Anlage 28

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

Anlage 29

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 in Wiesbaden

Datenschutz nach „Charlie Hebdo“ : Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Anlage 30

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (siehe BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Anlage 31

Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. August 2015

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 15. Juni 2015 seinen Standpunkt zur Datenschutz-Grundverordnung abgeschlossen hat, beraten Kommission, Parlament und Rat seit Ende Juni im sogenannten Trilog über ihre verschiedenen Positionen zur Datenschutz-Grundverordnung mit dem Ziel einer Gesamteinigung und Verabschiedung des Rechtsaktes zum Jahresende 2015.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Sie hat sowohl zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben als auch in einer Reihe von Entschließungen und Stellungnahmen zu einzelnen Fragen der Datenschutzreform Position bezogen[1]. Die Konferenz hat von Anfang an das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“[2]. Dies gilt umso mehr, als die Kommission ausdrücklich das Grundrecht des Einzelnen auf Datenschutz in den Mittelpunkt gerückt hat, dem die Reform zugutekommen soll.

Deshalb ist es für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand – der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist – einen verbesserten, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Keinesfalls darf die Reform des Europäischen Datenschutzrechts dazu führen, hinter dem geltenden Datenschutzniveau zurückzubleiben. Die Konferenz betont, dass die sich aus Art. 8 der Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes daher nicht zur Disposition stehen dürfen. Nach wie vor fehlen spezifische Anforderungen an riskante Datenverarbeitungen, wie z. B. beim Profiling oder bei der Videoüberwachung. Auch sollen Daten für Werbezwecke weiterhin ohne Einwilligung der Betroffenen verarbeitet werden können. Gerade in Zeiten von Big Data und globaler Datenverarbeitung

---

[1] Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 sowie Stellungnahme vom 11.6.2012; „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012; „Europa muss den Datenschutz stärken“ nebst Erläuterungen vom 13./14.3.2013; „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28.3.2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 18./19.3.2015, jeweils abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBundLaender/Functions/DSK_table.html

[2] Mitteilung der Kommission „Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“, KOM(2012) 9 endg., Ziff. 6

sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Bei den genannten und den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der Datenschutz-Grundverordnung.

II. Die Vorschläge im Einzelnen

1. Der Anwendungsbereich der Datenschutz-Grundverordnung

a. Keine Ausweitung der Haushaltsausnahme!

Der Rat hat die so genannte Haushaltsausnahme in Art. 2(2)(d) Datenschutz-Grundverordnung (DSGVO) in der Weise erweitert, dass er die im Kommissionsvorschlag enthaltenen Worte „ausschließlich“ und „ohne jede Gewinnerzielungsabsicht“ gestrichen hat.

Der Vorschlag des Rates ist in einer Weise formuliert, dass ein maßgeblicher Teil der Verarbeitung personenbezogener Daten durch natürliche Personen auch dann aus dem Anwendungsbereich des Datenschutzrechts herausfiele, wenn in erheblicher Weise in das Datenschutzgrundrecht Dritter eingegriffen würde. Nach der Formulierung des Rates würde es bereits genügen, wenn die Verarbeitung zu persönlichen oder familiären Zwecken bei einer Gesamtbetrachtung lediglich einen völlig untergeordneten Zweck darstellte, um unter die Haushaltsausnahme zu fallen und damit nicht mehr dem Datenschutzrecht zu unterliegen. Ein Nutzer eines sozialen Netzwerks oder der Betreiber einer privaten Homepage würde selbst dann nicht unter das Datenschutzrecht fallen, wenn er in großem Umfang personenbezogene Daten unbeschränkt im Internet veröffentlicht, solange er die Datenverarbeitung (auch) als eine solche zu persönlichen oder familiären Zwecken deklariert. Eine derartige Erweiterung wäre nicht akzeptabel. Ebenso wenig kann die Gewinnerzielungsabsicht ein Kriterium für die Anwendung des Datenschutzrechts sein, da die Eingriffstiefe einer Datenverarbeitung hiervon nicht abhängt. Eine zu weitgehende Ausdehnung der Haushaltsausnahme stünde im Widerspruch zum primärrechtlich garantierten Grundrecht auf Datenschutz und kann deshalb im Sekundärrecht nicht umgesetzt werden.

Die Konferenz spricht sich gegen eine Erweiterung der Haushaltsausnahme in Art. 2(2)(d) DSGVO und die damit verbundene Einschränkung des Anwendungsbereichs des Datenschutzrechts aus. Die Haushaltsausnahme sollte sich daher weiterhin an dem Wortlaut von Art. 2(2) der Richtlinie 95/46/EG orientieren und nur solche Verarbeitungsvorgänge aus dem Anwendungsbereich herausnehmen, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

b. Keine weitere Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie!

Die DSGVO wird keine Anwendung finden, soweit die Richtlinie für den Bereich Polizei und Justiz (JI-RL) Anwendung finden wird. Somit bestimmt der Anwendungsbereich der JI-RL zugleich den Anwendungsbereich der DSGVO. Vor diesem Hintergrund hat der Rat in den letzten Monaten verschiedene Entwürfe diskutiert, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-RL führen könnten.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche von DSGVO und der JI-RL wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der KOM enthält die JI-RL Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst ist, soweit sie der Prävention einer Straftat dient. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizeien unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-RL – zusammenzufassen, soll der Anwendungsbereich der RL entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die RL zu fassen.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern überhaupt ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-RL für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen zumindest sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Die Datenverarbeitung von anderen Behörden muss weiterhin von der DSGVO geregelt werden, wie es auch der gegenwärtige Rechtsrahmen vorsieht.

Die Konferenz spricht sich gegen die in der Ratsfassung hinzugefügte Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie in Art. 2(2)(e) DSGVO aus. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DSGVO geregelt werden.

2. Für eine klare Definition des Personenbezugs!

Die DSGVO knüpft wie auch das geltende Recht weiterhin am Begriff des personenbezogenen Datums an. Dies ist die logische Konsequenz aus der grundrechtlichen und primärrechtlichen Gewährleistung in Art. 8 Abs. 1 EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden Daten hat. Deshalb kommt der Definition des personenbezogenen Datums in Art. 4(1) DSGVO eine außerordentlich hohe Bedeutung zu, denn sie entscheidet letztlich über die Anwendbarkeit des Datenschutzrechts.

Dabei muss klargestellt sein, dass eine natürliche Person auch dann als identifizierbar anzusehen ist, wenn sie innerhalb einer Gruppe von Personen von anderen Personen unterschieden und damit auch unterschiedlich behandelt werden kann. Des-

halb muss die Identifizierbarkeit einer Person auch deren Herausgreifen einschließen, wie es dem Vorschlag des Parlaments in EG 23 zugrundeliegt.

Die Vorschläge von Kommission und Rat zu EG 24 führen zudem zu einer unnötig restriktiven Auslegung des Begriffs des personenbezogenen Datums, indem sie Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten ansehen. Für diese Daten gelten die gleichen Kriterien für die Bestimmung des Personenbezugs wie für jede andere Information. Deren gesonderte Erwähnung verleitet zu dem unzulässigen Schluss, dass hier andere Kriterien gelten würden. Dies widerspräche auch der Rechtsprechung des EuGH.

Die Konferenz unterstützt insoweit den Vorschlag des Parlaments zu EG 23, wonach klargestellt ist, dass die Möglichkeit des Herausgreifens einer natürlichen Person aus einer Gruppe ein Mittel zu deren Identifizierbarkeit ist.

Die Konferenz fordert, bei EG 24 dem Vorschlag des Parlaments zu folgen, der klarstellt, dass Kennnummern, Standortdaten, Online-Kennungen, IP-Adressen oder sonstige Elemente grundsätzlich als personenbezogene Daten zu betrachten sind.

3. Datensparsamkeit muss Gestaltungsziel bleiben!

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten. Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Gerade deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je. Auf diese Weise werden Anreize für eine datenschutzfreundliche Gestaltung von Verarbeitungs- und Geschäftsprozessen geschaffen.

Dies haben die Kommission und das Parlament erfreulicherweise auch erkannt, indem sie das Prinzip der Datensparsamkeit ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5(1)(c) DSGVO verankert haben. Umso unverständlicher ist es, dass der Rat in seinem Entwurf das Prinzip der Datenvermeidung aus dem Text gestrichen hat – ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten.

Die Konferenz spricht sich für eine ausdrückliche Verankerung des Prinzips der Datensparsamkeit in Art. 5(1)(c) DSGVO entsprechend der Formulierung der Kommission bzw. des Parlaments aus.

4. Keine Aufweichung der Zweckbindung!

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der

Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.

Dementsprechend folgt der Kommissionsentwurf der DSGVO grundsätzlich dem hergebrachten Ansatz der Richtlinie 95/46/EG, indem er in Art. 5(1)(b) zunächst festlegt, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Die Konzeption der geltenden Richtlinie 95/46/EG ist dadurch geprägt, dass sie eine Verarbeitung personenbezogener Daten zu anderen Zwecken nur zulässt, wenn diese neuen Zwecke mit dem Ursprungszweck vereinbar sind. Weitere Zweckänderungen lässt die Richtlinie nicht zu. Auf dieser Basis ist es in der Regel gelungen, einen starken Schutz des Rechts auf informationelle Selbstbestimmung in einen angemessenen Ausgleich mit den öffentlichen Datenverarbeitungsinteressen des Staates und den legitimen Interessen der Unternehmen zu bringen.

Hiervon abweichend hat die Kommission in ihrem Vorschlag zu Art. 6(4) DSGVO zusätzlich die Möglichkeit vorgesehen, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Verarbeitungszweck nicht vereinbar sind. Der Rat hat diese Ausnahme noch erweitert, indem er solche Zweckänderungen auch bei einem überwiegenden berechtigten Interesse des Verarbeiters zulassen will. Spätestens durch diese Ergänzungen werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

Das Europäische Parlament ist deshalb zu dem bewährten Ansatz der Richtlinie 95/46/EG zurückgekehrt und hat konsequenterweise Art. 6(4) DSGVO gestrichen. Dies entspricht auch einer frühzeitig erhobenen Forderung der Artikel-29-Gruppe der Europäischen Datenschutzbehörden.

Die Gewährleistung einer starken Zweckbindung ist eine unabdingbare Voraussetzung, um dem Einzelnen ein Höchstmaß an Entscheidungsfreiheit und Transparenz zu ermöglichen. Die Konferenz lehnt deshalb die vom Rat vorgeschlagene Aufweichung der Zweckbindung entschieden ab und spricht sich auf der Basis des Ratsvorschlages für eine Streichung des Art. 6(4) DSGVO aus.

5. Keinen datenschutzrechtlichen Freibrief für Statistik, Archive sowie wissenschaftliche und historische Zwecke!

Die Verarbeitung personenbezogener Daten für die im öffentlichen Interesse tätigen Archive, für die Statistik sowie für historische und für Forschungszwecke folgt aufgrund der jeweiligen Eigenarten der genannten Zweckbestimmungen zum Teil besonderen Regelungen. In allen Fällen geht es darum, die Grundrechte auf Datenschutz und Privatsphäre in einen angemessenen Ausgleich zu bringen mit wichtigen – zum Teil ebenfalls grundrechtlich – geschützten Interessen wie der Forschungs-

freiheit oder den öffentlichen Interessen an der amtlichen Statistik bzw. der langzeitlichen Verfügbarmachung staatlicher Informationen durch die Archive. Dies wird grundsätzlich auch durch die Datenschutzbeauftragten des Bundes und der Länder anerkannt. Das geltende Datenschutzrecht hat diesen Ausgleich bisher angemessen hergestellt.

Der Rat geht in seinem Entwurf in verschiedener Hinsicht über diesen Ansatz hinaus und privilegiert die genannten Bereiche in unannehmbarer Weise. Einerseits soll eine Weiterverarbeitung zu den genannten Zwecken gem. Art. 5(1)(b) DSGVO generell immer möglich sein; die Zweckbindung wird insoweit aufgehoben. Andererseits soll Art. 6(2) DSGVO die (Weiter-)Verarbeitung zu den genannten Zwecken ermöglichen, ohne dass es der Rechtsgrundlagen des Art. 6(1) DSGVO bedarf. Dies würde bedeuten, dass eine Verarbeitung zu den genannten Zwecken ohne weitere Rechtsgrundlage – vorbehaltlich mitgliedsstaatlicher Sonderbestimmungen in Teilbereichen nach Art. 83 DSGVO – möglich wäre und die Weiterverarbeitung personenbezogener Daten, die ursprünglich zu anderen Zwecken erhoben worden sind, weitgehend schrankenlos möglich wäre.

Hinzu kommt, dass der gegenständliche Anwendungsbereich der Privilegierung zu weit gefasst ist. Einzig für die Archive im öffentlichen Interesse bestehen insofern keine Bedenken, zumal sich zumindest die staatlichen Archive nach Art. 83 DSGVO nach dem meist ausdifferenzierten mitgliedsstaatlichen Recht zu richten haben. Bei der Privilegierung der statistischen Zwecke differenziert der Ratsentwurf hingegen nicht nach solchen der amtlichen Statistik und sonstigen statistischen Zwecken. Während für erstere im Rahmen von Art. 83 DSGVO eine Privilegierung nachvollziehbar ist, besteht im Übrigen die Gefahr, dass etwa die Betreiber von sozialen Netzwerken, Suchmaschinen, Analysetools usw. die von ihnen vorgenommene umfassende Profilbildung als statistische Zwecke deklarieren. Vergleichbare Bedenken bestehen auch gegen die Privilegierung der wissenschaftlichen Datenverarbeitung, die vom Rat nicht auf Zwecke der wissenschaftlichen Forschung beschränkt wird, sondern darüber hinausgeht.

Datenschutzrechtliche Grundsätze gelten auch für die Verarbeitung personenbezogener Daten zu Zwecken der öffentlichen Archive, der Statistik sowie für wissenschaftliche und historische Zwecke. Die Konferenz erwartet im Trilog eine differenzierte und ausgewogene Regelung zum Schutze der genannten Interessen, die die Einschränkungen der Grundrechte auf Datenschutz und Privatsphäre auf das unabdingbar Notwendige beschränkt. Jede Verarbeitung zu den genannten Zwecken bedarf einer Rechtsgrundlage im Sinne von Art. 6(1) DSGVO. Art. 6(2) DSGVO ist insofern missverständlich und sollte daher gestrichen werden. Darüber hinaus sollte – vergleichbar mit den Archiven – nur die amtliche Statistik privilegiert werden. Profilbildungen in sozialen Netzwerken, Suchmaschinen, durch den Einsatz von Analysetools usw. dürfen nicht privilegiert werden.

6. Die Einwilligung muss die Datenhoheit des Einzelnen sichern!

Recht auf informationelle Selbstbestimmung bedeutet seit jeher, dass der Einzelne grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden darf. Daraus folgt unmittelbar, dass der Einzelne grundsätzlich autonom darüber bestimmen kann, ob er eine Verarbeitung seiner personenbezogenen Daten erlaubt oder nicht.

Die Einwilligung ist ein wesentliches Element, um diese Autonomie wirksam zu sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Nur bei einer ausdrücklichen Willensbekundung kann letztlich der Nachweis erbracht werden, dass sich der Einzelne der Tragweite seiner Entscheidung bewusst wird.

Der Rat verabschiedet sich in seinem Entwurf entgegen der Grundrechtecharta von diesem Grundsatz, indem er bereits eine eindeutige Willensbekundung ausreichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Als datenschutzgerechte Einwilligung kann nur ein opt-in akzeptiert werden.

Es sollte zudem ein Koppelungsverbot ausdrücklich in den verfügenden Teil der DSGVO aufgenommen werden. Während Kommission und Parlament dieses in Art. 7(4) DSGVO vorsehen, hat es der Rat gestrichen und erwähnt es lediglich in den Erwägungsgründen (EG 34).

Zur wirksamen Gewährleistung des Rechts auf informationelle Selbstbestimmung unterstützt die Konferenz den Ansatz von Kommission und Parlament, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird. In Art. 7 DSGVO sollte darüber hinaus ein Koppelungsverbot ausdrücklich geregelt werden.

7. Rechte der Betroffenen

a. Sicherstellung der Unentgeltlichkeit

Die Entwürfe der Kommission und des Parlaments sehen in Art. 12(4) DSGVO vor, dass Unterrichtungen der Betroffenen und die auf Antrag ergriffenen Maßnahmen zur Umsetzung der Betroffenenrechte unentgeltlich sind. Der Entwurf des Rates sieht dagegen vor, dass lediglich die Informationen gemäß Art. 14 und 14a sowie alle Mitteilungen gemäß den Art. 16 bis 19 und 32 unentgeltlich zur Verfügung gestellt werden. Damit bleibt unklar, ob auch die Umsetzung der Betroffenenrechte selbst unentgeltlich erfolgen muss oder die verantwortlichen Stellen hierfür ggf. eine Gebühr erheben können. Dafür spricht, dass nur das Auskunftsrecht (Art. 15) ausdrückliche Regelungen zur (Un-)Entgeltlichkeit enthält (vgl. Art. 15(1) und (1b)), die übrigen Betroffenenrechte hingegen nicht.

Die Unentgeltlichkeit der Ausübung und Umsetzung der Betroffenenrechte ist unabdingbare Voraussetzung für die effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Gebühren für die Ausübung schrecken die Betroffenen regelmäßig von der Wahrnehmung ihrer Rechte ab.

Die Konferenz spricht sich für eine unmissverständliche Regelung aus, dass die Ausübung der Betroffenenrechte und deren Umsetzung durch die verantwortlichen Stellen unentgeltlich erfolgen müssen.

b. Keine Einschränkung der Betroffenenrechte!

Die Information der Betroffenen (Art. 14, 14a DSGVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Entwurf des Rates sieht lediglich die Unterrichtung über die Identität der verantwortlichen Stelle, die Zwecke der Datenverarbeitung und die Rechtsgrundlage vor. Weitergehende Informationen sollen nur dann erforderlich sein, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Die Konferenz lehnt Beschränkungen der Betroffenenrechte ab. Die Formulierungen des Rates führen zu Rechtsunsicherheit und lassen Raum für Interpretationen, die zu einer Absenkung des geltenden Datenschutzniveaus führen.

Die Informationspflichten der Art. 14 und 14a DSGVO beinhalten im Gegensatz zum Recht auf Auskunft (Art. 15) lediglich allgemeine, abstrakte Informationen über Art, Umfang und Zweck der Datenverarbeitung. Die Informationspflicht führt daher nicht zu exzessiven Bürokratiekosten, weil sie in standardisierter Form gegenüber den Betroffenen erfüllt werden kann. Die vom Europäischen Parlament vorgeschlagenen standardisierten Informationsmaßnahmen unter ergänzender Verwendung von Piktogrammen (Art. 13a) erachtet die Konferenz für erwägenswert.

Die Konferenz spricht sich gegen Einschränkungen der Betroffenenrechte aus und unterstützt die Position des Europäischen Parlaments.

c. Wirksame Begrenzung der Profilbildung sicherstellen!

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, dass die bisherigen Vorschläge für eine Regelung von Profilbildungen in Art. 20 DSGVO nicht geeignet sind, um die Bürgerinnen und Bürger im Zeitalter von Big Data, der Allgegenwart des Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Die Vorschläge von Kommission, Parlament und Rat zu Art. 20 DSGVO sind unzureichend, da keiner der Vorschläge die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen unterwirft, sondern erst das Treffen einer „automatisierten Entscheidung“ (Rat) oder einer „Maßnahme“ (KOM) auf Basis des Profilings bzw. „Profiling, das Maßnahmen zur Folge hat, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Interessen der betroffenen Person hat“ (EP).

Unzulänglich ist insbesondere der Vorschlag des Rates, da er das Phänomen des Profilings in Anlehnung an Art. 15 Abs. 1 der EG-Datenschutzrichtlinie 95/46 auf das Treffen automatisierter Entscheidungen mit Rechtswirkung für den Einzelnen redu-

ziert. Geregelt wird damit lediglich eine spezifische Folge der Datenverarbeitung im Zusammenhang mit der Auswertung von Persönlichkeitsmerkmalen, nicht aber die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Vor diesem Hintergrund plädieren die Datenschutzbeauftragten des Bundes und der Länder für eine differenzierte Regelung der Profilbildung und -nutzung in der DSGVO, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst. Diesem Ansatz entspricht am ehesten der vom Europäischen Parlament zu Art. 20 unterbreitete Regelungsvorschlag.

- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Wegen ihrer hohen Sensitivität sollte zudem festgelegt werden, dass besondere Kategorien personenbezogener Daten nicht in eine Profilbildung einfließen dürfen.

- In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss wissen, wann, zu welchem Zweck und in welcher Form seine Daten im Internet oder bei der Nutzung eines Dienstes auf einem Endgerät zu Profilingzwecken verarbeitet werden und muss hierzu seine ausdrückliche Einwilligung erteilen.

- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen, letzteres flankiert von einem Verbot der (Re-)Identifizierung.

In Anbetracht der wiederholt vom EuGH festgestellten Gefahren, die von Persönlichkeitsprofilen für das Grundrecht auf Datenschutz ausgehen, fordert die Konferenz, die vorliegenden Vorschläge für eine Profilingregelung im Sinne der vorgenannten Eckpunkte substanziell zu verbessern.

8. Die datenschutzrechtliche Verantwortlichkeit gilt für jede Verarbeitung personenbezogener Daten!

Die in Kapitel IV, insbesondere in Art. 22 DSGVO geregelte Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen (*Accountability*) gehört zu den zentralen Grundprinzipien eines modernen Datenschutzrechts. Die für die Verarbeitung Verantwortlichen und die Auftragsdatenverarbeiter sind in jedem Falle und ohne Einschränkungen für die Einhaltung des Datenschutzrechts verantwortlich. Dies gilt ungeachtet der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen.

Ebenso müssen die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter uneingeschränkt in der Lage sein, die Einhaltung ihrer Pflichten nachzuweisen. Risikobasierte Aspekte dürfen lediglich bei der Frage berücksichtigt werden, welche konkreten Maßnahmen zur Einhaltung der Pflichten zu treffen sind.

Es muss daher klargestellt werden, dass sich ein risikobasierter Ansatz nicht auf das „Ob“ und die Nachweisbarkeit, sondern allenfalls auf das „Wie“ der Einhaltung der Pflichten beziehen kann. Dies wird im Vorschlag der Kommission am besten verdeutlicht, in dem auf jede Relativierung verzichtet wird.

Die Konferenz spricht sich für den seitens der Kommission für Art. 22 DSGVO gewählten Ansatz aus, um zu verdeutlichen, dass die Verantwortlichkeit („Accountability“) ein tragendes Grundelement des Datenschutzes ist, das als solches einem risikobasierten Ansatz nicht zugänglich ist.

9. Für die Verankerung von Gewährleistungszielen beim technischen und organisatorischen Datenschutz!

Die Verarbeitung personenbezogener Daten bedarf zum Schutz der Grundrechte nicht nur eines rechtlichen, sondern auch eines technischen und organisatorischen Schutzes. Ein modernes Datenschutzrecht muss hierfür Gewährleistungsziele definieren, an denen sich die zu treffenden Maßnahmen auszurichten haben. Dies bedeutet, dass zu den klassischen Gewährleistungszielen der IT-Sicherheit spezifische Ziele hinzutreten müssen, die sich namentlich auf den Schutz personenbezogener Daten beziehen. Deshalb sind die Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, aber auch Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in der DSGVO zu verankern. Während sich Kommission und Rat in ihren Vorschlägen zu Art. 30(2) bzw. 30(1a) DSGVO im Wesentlichen auf die klassischen Ziele Verfügbarkeit, Integrität und Vertraulichkeit fokussieren, geht der Ansatz des Parlaments in Art. 30(1a) und 30(2) DSGVO i. V. m. Art. 5(1)(ea) und (eb) am weitesten.

Die Konferenz hält eine konsequente, klare und übersichtliche Verankerung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in Art. 30 DSGVO für notwendig. Sie unterstützt insoweit die Zielrichtung des Parlaments, spricht sich allerdings für eine übersichtlichere Gestaltung aus.

10. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Ungeachtet der materiell-rechtlichen Bestimmungen hängt das konkrete Datenschutzniveau in Behörden und Unternehmen ganz entscheidend davon ab, welche Akzeptanz der Datenschutz vor Ort genießt und wie die Datenschutzkultur ausgeprägt ist. Hierzu können die Aufsichtsbehörden für den Datenschutz Impulse liefern und durch Kontrollen und Beratungen einen entscheidenden Beitrag leisten. Diese Aktivitäten bleiben aber notwendigerweise punktuell und sind aufgrund der unterschiedlichen Rollen nicht immer konfliktfrei. Deshalb kommt der Institution der Datenschutzbeauftragten in Unternehmen und Verwaltungen eine hohe Bedeutung zu.

Es ist deshalb erfreulich, dass sowohl Kommission als auch Parlament in Art. 35 DSGVO die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen.

Allerdings sind die von beiden Institutionen gewählten Kriterien, unter denen eine Bestellung verpflichtend ist, wenig überzeugend.

Bedauerlicherweise hat sich im Rat eine europaweit geltende Verpflichtung zur Bestellung von Datenschutzbeauftragten nicht durchgesetzt. Hierbei wird vor allem mit dem bürokratischen und wirtschaftlichen Aufwand argumentiert. Nach den jahrzehntelangen Erfahrungen in Deutschland überzeugt dieses Argument nicht. Der Compliance-Aufwand für die Unternehmen ist ohne die Einbindung betrieblicher Datenschutzbeauftragter nicht unerheblich; durch deren Einsatz können zudem Sanktionen und Bußgelder oftmals vermieden werden.

Die Konferenz setzt sich nach wie vor dafür ein, dass eine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter europaweit verbindlich vorgeschrieben wird. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

11. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten!

Seit den Enthüllungen von Edward Snowden wird intensiv über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43a DSGVO vorgeschlagen. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten zuständigen Stellen.

Die Konferenz unterstützt diese Forderung ebenso wie die Artikel-29-Gruppe. Mit der Schaffung einer solchen Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Der Rat ist einer entsprechenden Initiative der Bundesregierung bedauerlicherweise nicht gefolgt.

Die Konferenz spricht sich weiterhin dafür aus, eine spezifische Rechtsgrundlage für die Datenübermittlung an Behörden und Gerichte in Drittstaaten zu schaffen, mit der insbesondere im Hinblick auf die nachrichtendienstliche Überwachung mehr Transparenz und Kontrolle geschaffen wird. Sie unterstützt den vom Parlament eingebrachten Vorschlag eines Art. 43a DSGVO.

Die Zuständigkeit sollte jedoch wie folgt geregelt werden: Haben ersuchender und ersuchter Staat ein Rechtshilfeabkommen oder einen ähnlichen internationalen Ver-

trag geschlossen, sollte die hierin bezeichnete Stelle für die Entgegennahme und Prüfung eines Ersuchens auf Datenübermittlung zuständig sein. In den Fällen, in denen eine zuständige Stelle nicht vertraglich bestimmt worden ist, kann diese Aufgabe nachrangig in die Zuständigkeit der Datenschutzaufsichtsbehörden fallen.

12. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Um dies zu gewährleisten und auf der anderen Seite den Unternehmen einen Mehrwert zu bieten, hatte die Kommission einen sog. One-Stop-Shop, einen Kohärenzmechanismus und die Einrichtung eines Europäischen Datenschutzausschusses vorgeschlagen.

Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten. Das vom Rat vorgeschlagene Modell ist für die Aufsichtsbehörden komplex, soll aber den Bürgerinnen und Bürgern eine ortsnahe Bearbeitung ihrer Anliegen und den Unternehmen einen Ansprechpartner für länderübergreifende Datenverarbeitungen verschaffen.

Die Konferenz unterstützt die Ziele des Ratsvorschlags zum sog. One-Stop-Mechanismus. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedsstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt.

Der One-Stop-Shop soll einen ausgewogenen Ausgleich zwischen den verschiedenen Interessen schaffen, eine bürgernahe Bearbeitung von Beschwerden ermöglichen, den Unternehmen klare Ansprechpartner zur Verfügung stellen und durch die Aufwertung des Europäischen Datenschutzausschusses die notwendige Verbindlichkeit und damit Rechtssicherheit aufweisen. Die Konferenz bittet die am Trilog beteiligten Parteien gleichwohl, praktikable Verfahrensregeln festzulegen. Dies betrifft insbesondere die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander.

13. Für einen starken Beschäftigtendatenschutz

Die DSGVO überlässt die Regelung des Datenschutzes für Beschäftigte in Art. 82 dem mitgliedsstaatlichen Recht. Der Rat und die Kommission legen fest, dass die Mitgliedstaaten dabei den Rahmen der DSGVO einhalten müssen und verzichten auf

konkretere Anforderungen. Das Europäische Parlament gibt dagegen ganz konkrete Mindeststandards im Verordnungstext vor.

Die Konferenz hält es für wichtig, dass Art. 82 DSGVO den Mitgliedstaaten in jedem Falle die Möglichkeit eröffnet, auch über den Standard der DSGVO hinausgehen zu können. Die Konferenz begrüßt den Ansatz des Parlaments, konkrete Mindeststandards für den Beschäftigtendatenschutz im Verordnungstext selbst vorzusehen.

Im Kontext der Verarbeitung von Beschäftigtendaten sollte es die Datenschutz-Grundverordnung den Mitgliedstaaten ermöglichen, im Sinne einer Mindestharmonisierung auch über das Datenschutzniveau der Verordnung hinauszugehen. Die Konferenz unterstützt den Ansatz des Parlaments, konkrete Mindeststandards festzulegen.

14. Recht auf pseudonyme Internet-Nutzung für alle Menschen in Europa schaffen!

Es gibt zahlreiche gewichtige Gründe, bei der Nutzung von Telemediendiensten auf ein Pseudonym zurückzugreifen: Dazu gehört etwa der Wunsch, einer Profilbildung unter dem realen Namen zu entgehen, sei es um sich vor rechtswidrigen Zugriffen zu schützen, sei es zur Stärkung des Schutzes bei der Nutzung sozialer Netzwerke. Ein Pseudonym kann ferner vor politischer oder rassistischer Verfolgung oder Diskriminierung und sozialer Benachteiligungen etwa wegen der sexuellen Ausrichtung schützen. Pseudonyme können schließlich verhindern, dass die private Nutzung eines Telemediums zur geschäftlichen Kontaktaufnahme durch Dritte missbraucht wird. Das ist gerade bei Berufsgeheimnisträgern wie Ärzten, Seelsorgern, Anwälten oder Sozialarbeitern nicht zuletzt zum Schutz der mit ihnen in Kontakt stehenden Personen von Bedeutung.

Das Recht, in Telemedien grundsätzlich auch unter einem Pseudonym gegenüber anderen Nutzern aufzutreten, stärkt sowohl die informationelle Selbstbestimmung Betroffener als auch die Meinungsfreiheit, ohne eine Verfolgung und Ahndung von missbräuchlichem Verhalten von unter Pseudonym auftretenden Nutzern durch den Telemedienanbieter auszuschließen. In der Europäischen Datenschutzgrundverordnung fehlt jedoch im Katalog der Rechte Betroffener eine entsprechende ausdrückliche Regelung.

Die Konferenz hält es für erforderlich, zum Schutz der Privatsphäre der Telemediennutzer eine Bestimmung aufzunehmen, die zumindest bei zu privaten Zwecken genutzten Telemedien innerhalb der EU ein Recht auf pseudonyme Nutzung verbindlich statuiert.

Anlage 32

Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30. September und 1. Oktober 2015 in Darmstadt

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

Anlage 33

Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30. September und 1. Oktober 2015 in Darmstadt

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Ein Opt-Out reicht auf Basis von AGB und datenschutzunfreundlichen Voreinstellungen nicht aus, um weitreichende Datenverarbeitungsbefugnisse zu schaffen. Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

Anlage 34

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 29. Oktober 2015

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 9. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DSGVO) im Paket zum Jahresende 2015.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012[1] mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August 2015 hat sie zu den Trilogverhandlungen zur DSGVO Stellung genommen[2]. Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben[3]. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“ und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im Anwendungsbereich der JI-Richtlinie hingewiesen. Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert[4].

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

---

[1] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

[2] Trilogpapier der Konferenz zur DSGVO, abrufbar unter: https://www.datenschutz.hessen.de/entschliessungen.htm

[3] Stellungnahmen zur DSGVO und zur JI-Richtlinie vom 11.6.2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012, jeweils abrufbar unter https://www.datenschutz.hessen.de/entschliessungen.htm und https://www.datenschutz.hessen.de/taetigkeitsberichte.htm

[4] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 3.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI-Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DSGVO. Denn die DSGVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit“ erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DSGVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die

JI-Richtlinie Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-Richtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DSGVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DSGVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DSGVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf“. Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden[5].

Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine

[5] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 5.

Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar“ mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).

Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff“)[6].

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtiger Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert.

Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments

[6] BVerfGE 100, 313, 389; ständige Rechtsprechung.

nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records“, Art. 23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten“ der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen) Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Demgegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltschaftlichen Verfahrensakten die Regelung, dass die Ausübung der Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht“ erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt des Art. 17 JI-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der JI-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 JI-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwaltschaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung – Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 JI-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie“. Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar“ sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik“ („state of the art“) sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der JI-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare“ Technik bzw. Technologie sollte konsequenter Weise auch in der JI-Richtlinie durch „Stand der Technik“ ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25a (2) lit. b erwähnten „biometrischen Daten“ gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinienvorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der

Definition der „biometrischen Daten“, wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art. 35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in internationalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Ver-

hältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentationspflicht gem. Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV verlangen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die JI-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Düsseldorfer Kreis

Anlage 35

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 11. und 12. September 2013

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z. B. §§ 28 und 32 BDSG) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

Anlage 36

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 27. Januar 2014

Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“[1] zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

[1] http://www.datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Service/orientierungshilfen/OH_SelbstauskunftMietinteressenten.pdf

Anlage 37

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 25. und 26. Februar 2014

Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, sodass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

Anlage 38

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 25. und 26. Februar 2014

Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,

- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),

- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,

- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne Weiteres dem Zertifikat entnehmen können,

- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,

- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

Anlage 39

Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten vom Mai 2014

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV- Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

    - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

    - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.

- Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.

- Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

Europäische Datenschutzkonferenz

Anlage 40

Entschließung der Konferenz der europäischen Datenschutzbeauftragten vom 5. Juni 2014 in Straßburg

Überarbeitung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108)

– Übersetzung –

Bei vergangenen Frühjahrskonferenzen haben die europäischen Datenschutzbehörden wiederholt ihre Absicht zum Ausdruck gebracht, aktiv an der Entwicklung des Datenschutzes innerhalb und außerhalb Europas mitzuwirken und hohe Standards in diesem Bereich zu fördern.[1]

Im Bewusstsein der großen Herausforderungen und Risiken, die sich durch die technischen Entwicklungen und durch die zunehmende Tendenz von Regierungen ergeben, eine Massenüberwachung von Personen durchzuführen, unterstreicht die Konferenz die Notwendigkeit, die verschiedenen Rechtsrahmen zum Datenschutz auf der Grundlage bestehender Prinzipien zu modernisieren und zu stärken.

Die Globalisierung der Datenverarbeitung und des Datenaustauschs erfordert einen umfassenden Ansatz unter Berücksichtigung des europäischen und des internationalen Rechtsrahmens.[2]

Vor diesem Hintergrund unterstützt die Konferenz die Bemühungen des Europarats, das Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) sowie sein Zusatzprotokoll zu modernisieren, die beide allgemeine Grundsätze bekräftigen.

Die Konferenz lobt den Europarat dafür, Länder, die nicht Vertragsstaaten des Übereinkommens 108 und seines Zusatzprotokolls sind, zum Beitritt zu ermutigen, aber unterstreicht, dass die Bereitschaft zur Öffnung nicht zu einer Senkung des durch diese Instrumente geschaffenen hohen Datenschutzstandards führen darf.

In diesem Zusammenhang stellt die Konferenz fest, dass jede Absenkung des derzeit durch das Übereinkommen 108 und seines Protokolls gewährten Schutzes einen Rückschritt darstellen würde.

---

[1] Erklärung zur führenden Rolle und Zukunft des Datenschutzes in Europa, verabschiedet am 23. und 24. April 2009 in Edinburgh, Entschließung zur künftigen Entwicklung von Datenschutz und Privatsphäre, verabschiedet am 30. April 2010 in Prag.

[2] Entschließung über die Notwendigkeit eines umfassenden Rechtsrahmens für den Datenschutz, verabschiedet am 5. April 2011 in Brüssel.

Vor diesem Hintergrund fordert die Konferenz alle Mitgliedstaaten des Europarats und Vertragsstaaten des Übereinkommens 108 dazu auf, den derzeitigen durch das Übereinkommen gewährleisteten Schutz zu wahren und, wenn möglich, zu stärken und insbesondere die vom beratenden Ausschuss (T-PD) vorgeschlagenen Maßnahmen umzusetzen:

- Beibehaltung eines breiten Anwendungsbereichs, der jede Verarbeitung personenbezogener Daten im öffentlichen und privaten Sektor in der Zuständigkeit der Vertragsstaaten umfasst, damit jede Person unabhängig von ihrer Nationalität oder ihres Wohnorts das Recht auf den Schutz personenbezogener Daten hat;

- Begrenzung der Ausnahmeregelungen zu den Datenschutzgrundsätzen, wobei jede Ausnahme gesetzlich festgelegt, verhältnismäßig und in einer demokratischen Gesellschaft erforderlich sein muss;

- Eingruppierung genetischer und biometrischer Daten in die Kategorie „sensible Daten“;

- Einführung des Grundsatzes der Datenminimierung im Zusammenhang mit der Einhaltung des Verhältnismäßigkeitsprinzips;

- Gewährleistung, dass eine erforderliche Zustimmung zur Verarbeitung spezifisch, freiwillig und informiert ist und eine ausdrückliche Willensäußerung darstellt;

- Unterstreichung der Bedeutung der Transparenz, die den für die Verarbeitung Verantwortlichen dazu verpflichtet, die Personen, deren Daten verarbeitet werden, zumindest über seine Identität und die Zwecke der Verarbeitung, aber auch über die Datenempfänger und die Möglichkeiten zur Wahrnehmung ihrer Rechte zu unterrichten;

- Verbesserung der Rechte von Personen, insbesondere das Recht auf Zugang und Berichtigung sowie das Widerspruchsrecht;

- Aufnahme von Bestimmungen zur Regelung von Entscheidungen, die rein auf der automatischen Datenverarbeitung beruhen;

- Aufnahme von Rechenschaftspflichten, nach denen die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter bei allen Verarbeitungsschritten geeignete Maßnahmen ergreifen müssen, um die Einhaltung des Übereinkommens zu gewährleisten und nachzuweisen, und ab der Planungsphase der Verarbeitung den Datenschutz berücksichtigen müssen;

- Einführung einer Pflicht zur Meldung von Sicherheitsverstößen;

- Beibehaltung des hohen Schutzstandards für personenbezogene Daten und Aufsicht über internationalen Datentransfer im Interesse der Kohärenz und Einhaltung des Rechtsrahmens der Europäischen Union;

- Gewährleistung einer Evaluierung vor und nach der Ratifikation oder dem Beitritt zum Übereinkommen zur Prüfung der Existenz, Einhaltung und Effektivität von Maßnahmen zur Umsetzung der Bestimmungen des Übereinkommens.

Des Weiteren sollten Vertragsstaaten die Vertretung der Datenschutzbehörden im Beratenden Ausschuss von Übereinkommen 108 sicherstellen.

Schließlich stellt die Konferenz fest, dass ein effektiver Datenschutz die Schaffung unabhängiger Aufsichtsbehörden erfordert. In diesem Zusammenhang ist die Konferenz der Ansicht, dass Datenschutzbehörden zumindest folgende Befugnisse haben müssen:

- Ermittlungs- und Eingriffsbefugnisse sowie das Recht, Entscheidungen zu treffen und Sanktionen zu verhängen;

- Möglichkeit, Stellungnahmen zu allen Angelegenheiten des Datenschutzes abzugeben und insbesondere über alle rechtlichen oder administrativen Vorschläge zum Datenschutz konsultiert zu werden;

- Möglichkeit zur effektiven Zusammenarbeit durch den Austausch aller nützlichen Informationen und die Koordinierung ihrer Aktivitäten in einem Netzwerk.

Mit dieser Entschließung begrüßt die Konferenz die Vorschläge des Beratenden Ausschusses und fordert den Europarat auf, diese in seine Arbeit einzubeziehen. Die Konferenz unterstreicht, dass die Überarbeitung des Rechtsrahmens für den Datenschutz eine Möglichkeit darstellt, echte Verbesserungen beim Datenschutz vorzunehmen und einen effektiveren Schutz für jeden zu gewährleisten. In diesem Zusammenhang unterstreicht sie die Absicht der Datenschutzbehörden, untereinander und mit dem Europarat zu diesen Zielen eng zusammenzuarbeiten.

Anlage 41

Entschließung der Konferenz der europäischen Datenschutzbehörden vom 18. bis 20. Mai 2015 in Manchester, Vereinigtes Königreich

Erfüllung datenschutzrechtlicher Erwartungen in der digitalen Zukunft

– Übersetzung –

Vorschlagender:

The Information Commissioner's Office (ICO), Vereinigtes Königreich

Co-Sponsoren:

Garante per la Protezione dei Dati Personali, Italien
Commissão Nacional de Protecção de Dados, Portugal

Präambel

Die Welt hat sich seit der Annahme des Übereinkommens 108 des Europarates und der derzeitigen Europäischen Datenschutzrichtlinie 95/46 stark verändert. Die Einzelnen erwarten zu Recht, dass die Datenschutzbehörden auf diese Veränderungen eingehen. Neue Technologien und digitale Dienste entwickeln sich ständig weiter.

Immer mehr personenbezogene Daten werden auf immer komplexer werdende und potentiell einschneidendere Art und Weise erhoben, ausgetauscht und analysiert. Die Einzelnen verlassen sich immer stärker auf das Internet zur Durchführung von Transaktionen mit öffentlichen und privaten Einrichtungen, zum Zugriff auf Informationen und zur Interaktion mit anderen.

Im Rahmen dieser sich stetig wandelnden digitalen Welt, ihrer globalen Herausforderungen, der Aktualisierung des Übereinkommens Nr. 108 und des anstehenden Reformpakets zum Datenschutz in der EU werden die europäischen Datenschutzbehörden mit zahlreichen neuen Herausforderungen konfrontiert, mit Auswirkungen auf die Ausübung ihrer Aufgaben hinsichtlich der Förderung und Verteidigung der Datenschutzrechte.

Die Suche nach dem Ort von Privatsphärenschutz und Datenschutz gestaltet sich komplex. Manche Bürger mögen die Preisgabe ihrer personenbezogenen Daten als einen Teil des modernen Lebens akzeptiert haben, was aber noch nicht bedeutet, dass sie damit den Schutz der Privatsphäre aufgegeben haben. Es gibt überzeugende Belege dafür, dass in der Praxis viele Bürgerinnen und Bürger zunehmend über den Verlust der Kontrolle über ihre persönlichen Informationen besorgt sind, da die Systeme immer komplexer werden und die Nutzung dieser Systeme in der heutigen Gesellschaft unvermeidbar ist.

Trotz großer Sorge in der Öffentlichkeit über Privatsphäre und den Schutz personenbezogener Informationen, insbesondere in einem digitalen Umfeld, gibt es ein relativ geringes öffentliches Bewusstsein über die Existenz der Datenschutzbehörden und ihrer Schlüsselrolle für den Schutz des Datenschutzrechts der Einzelnen. Dies führt

nicht nur zu der Notwendigkeit, das Bewusstsein der Bürger für ihre Datenschutzrechte zu wecken, sondern auch das öffentliche Bewusstsein für die wichtige Rolle der Datenschutzbehörden hinsichtlich des Schutzes der personenbezogenen Daten.

Indessen werden die Datenschutzbehörden zunehmend mit finanziellen und anderen Ressourcenbeschränkungen konfrontiert, während gleichzeitig die Ansprüche an sie steigen. Nicht nur muss das Recht mit der sich stetig wandelnden digitalen Welt Schritt halten, sondern auch die Fähigkeit der Datenschutzbehörden für eine wirksame Aufsicht auf nationaler und EU-Ebene sowie auf einer breiteren europäischen Ebene. Wenn die Einzelnen notwendiges Vertrauen und Zuversicht für eine erfolgreiche digitale Zukunft haben sollen, dann müssen die den Datenschutzbehörden zur Verfügung stehenden Befugnisse und Ressourcenausreichend sein, damit sie in angemessener Weise für die Wahrung der Grundrechte und Freiheiten der Einzelnen im digitalen Zeitalter eintreten können.

Es ist aber nicht nur eine Frage der Ressourcen. Es ist ebenso notwendig, dass die Datenschutzbehörden einen nachhaltigen Ansatz auf nationaler, EU-weiter und auf einer breiteren europäische Ebene annehmen, damit sie ihre Aufgaben wahrnehmen können und ihre Tätigkeiten dort gezielt ausüben können, wo die Notwendigkeit des Schutzes der Privatsphäre am größten ist, und damit sie ein eingehendes Verständnis hinsichtlich der datenschutzrechtlichen Auswirkungen neuer und bestehender Technologien haben.

***

Die Europäische Konferenz der Datenschutzbehörden

- *In Anbetracht dessen*, dass das Zusatzprotokoll zum Übereinkommen Nr. 108 des Europarats anerkennt, dass die Aufsichtsbehörden ein notwendiger Bestandteil des wirksamen Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten sind, und dass diese Behörden zur Wahrung ihrer Effektivität in völliger Unabhängigkeit handeln und über die erforderlichen Befugnisse und Ressourcen verfügen müssen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

- *Auch unter Hinweis darauf*, dass in Art. 8 der Charta der Grundrechte der Europäischen Union das Recht auf den Schutz personenbezogener Daten vorgesehen ist, und dass dieses Recht die Kontrolle über die Einhaltung der datenschutzrechtlichen Vorschriften von einer unabhängigen Aufsichtsbehörde umfasst.

- *Ferner unter Hinweis darauf*, dass die kürzlich überarbeiteten OECD-Leitlinien für den Schutz der Privatsphäre bei grenzüberschreitendem Datenverkehr eine Bestimmung enthalten, wonach die Mitgliedstaaten Behörden zur Durchsetzung des Datenschutzes einrichten und aufrechterhalten sollten mit der für die wirksame Ausübung ihrer Befugnisse notwendigen Verwaltung sowie den nötigen Ressourcen und technologischen Fachkompetenzen.

- *Eingedenk entsprechend* der entscheidenden Rolle, die von starken, unabhängigen Datenschutzbehörden als Wächtern erwartet wird, wenn es um die

Wahrung der Grundrechte und Freiheiten der Einzelnen im digitalen Zeitalter geht.

- *In der Erwägung*, dass die Datenschutzbehörden ohne die notwendigen Befugnisse und Ressourcen nicht in der Lage sind, ihrer wichtigen Rolle nachzukommen, wozu auch ein besseres Verständnis für die Sorgen und Erwartungen der Einzelnen gehört, um ihnen einen wirksamen Schutz der Privatsphäre zu bieten.

- *In der Erkenntnis*, dass dies die Einzelnen zwangsläufig ohne ausreichenden Schutz lässt und dadurch Vertrauen und Zuversicht der Öffentlichkeit in eine digitale Zukunft gefährdet werden.

- *Unter Hinweis darauf*, dass der Gerichtshof der Europäischen Union[1] sich mit der Wichtigkeit von Finanzierung und Unabhängigkeit der Datenschutzbehörden befasst hat.

- *In dem Bewusstsein*, dass auf dem Papier stehende Rechte und Pflichten durchzusetzen und zu erbringen sind, da sie ansonsten im besten Fall eine Illusion und im schlimmsten Fall eine Täuschung der Bürgerinnen und Bürger darstellen.

1. **Fordert die Regierungen der europäischen Länder**[2] **auf**, dafür Sorge zu tragen, dass die finanzielle Ausstattung der Datenschutzbehörden zur Erfüllung ihrer ständig steigenden Anforderungen ausreichend ist, und dafür zu sorgen, dass die von den Gesetzgebern festgelegten Bestimmungen in der Praxis ordnungsgemäß befolgt werden. Dabei ist die Notwendigkeit der gegenseitigen Zusammenarbeit zu berücksichtigen, und dies muss auf eine Art und Weise erreicht werden, bei der die notwendige Unabhängigkeit respektiert und aufrechterhalten wird.

2. **Ruft die Gesetzgeber in ganz Europa zur Sicherstellung auf**, dass die nächste Generation der Datenschutzgesetze, soweit wie möglich, in klaren und einfachen Worten abgefasst wird, und dass sie von Organisationen, Einzelnen und Datenschutzbehörden auf einfache Weise verstanden und umgesetzt werden können, so dass sie das angestrebte hohe Datenschutzniveau so wirksam wie möglich in der Praxis umsetzen können.

3. **Erinnert die europäischen Datenschutzbehörden** an die Notwendigkeit:

- **ihre Anstrengungen zu erneuern** mit Blick auf die Sensibilisierung der Öffentlichkeit für Datenschutzrechte und auf die Sichtbarkeit der Arbeit der Datenschutzbehörden unter Berücksichtigung der steigenden Anforderungen und Herausforderungen;

---

[1] Europäische Kommission gegen Bundesrepublik Deutschland (C-518/07 vom 9. März 2010); Europäische Kommission gegen Republik Österreich (C-614/10 vom 16. Oktober 2012); Europäische Kommission gegen Ungarn (C-288/12 vom 8. April 2014).

[2] Der Begriff „europäische Länder“ umfasst nicht nur die Länder der Europäischen Union und des EWR, sondern auch Mitgliedstaaten des Europarates.

- **geeignete Methoden** zur bestmöglichen Nutzung ihrer begrenzten Ressourcen zu wählen, um wirkliche Ergebnisse für den Datenschutz der Einzelnen zu erzielen, insbesondere im Hinblick auf die Förderung der Entwicklung einer datenschutzfreundlichen digitalen Zukunft mittels technologisch integrierter Vorkehrungen zum Schutz der Privatsphäre;

- **der Zusammenarbeit** mit Dritten, einschließlich partnerschaftlicher Teilhabe unter den europäischen Datenschutzbehörden, mit der Internationalen Konferenz und anderen Dritten – etwa anderen Regulierungsbehörden, um sicherzustellen, dass das Thema Datenschutz so weit wie möglich durch die Arbeit anderer vorangebracht und ergänzt wird;

- **der Förderung** der Entwicklung datenschutzfreundlicher Mechanismen wie Datenschutzsiegel und Verhaltenskodizes zur Förderung der Befolgung und der guten Praxis - zur Ermöglichung eines „Strebens nach oben“ und zur Schaffung von Datenschutzvorschriften;

- **der Entwicklung** eines systematischen und proaktiven Ansatzes zur Bekämpfung von pflichtwidrigem Verhalten der für die Verarbeitung verantwortlichen Stellen, deren Tätigkeiten die größte Bedrohung für die Datenschutzrechte der Bürger darstellen;

- **der umso schnelleren Reaktion** auf neue Technologien und deren Auswirkungen auf den Datenschutz. Dies umfasst die kontinuierliche Entwicklung und den Austausch des internen technischen Fachwissens;

- **der Entschlossenheit**, wenn es um die Ressourcen für die Datenschutzbehörden geht, die diese zur effektiven Gewährleistung eines hohen Datenschutzniveaus für die Einzelnen benötigen. Dies umfasst die kontinuierliche Einflussnahme auf die Diskussion über das EU-Datenschutz-Reformpaket sowie auf Diskussionen über die Aktualisierung des Übereinkommens des Europarats Nr. 108 auf der Grundlage, dass die Gesetzgeber den Datenschutzbehörden bei der Wahrung der Grundrechte auf Privatsphäre und Datenschutz keine neuen Aufgaben auferlegen sollten, ohne ihnen gleichzeitig die vollständige Erfüllung dieser Aufgaben durch die Bereitstellung der erforderlichen Befugnisse und Ressourcen zu ermöglichen; und

- **der weiteren Entwicklung** von Initiativen, wie die Untergruppe für die Zusammenarbeit [Subgroup on Cooperation] der Artikel 29-Datenschutzgruppe und der Arbeitsgruppe der Frühjahrskonferenz für die Europäische Zusammenarbeit, die den Austausch von Informationen, Kenntnissen und Untersuchungen über praktische Herangehensweisen ermöglichen, die für die Datenschutzbehörden bei der Bewältigung ihrer zahlreichen Herausforderungen, mit denen sie konfrontiert werden, hilfreich sind.

Internationale Datenschutzkonferenz

Anlage 42

36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 13. bis 16. Oktober 2014 in Balaclava, Mauritius

Entschließung zum Datenschutz im digitalen Zeitalter

– Übersetzung –

Die 36. Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre

Verweist auf ihre Resolution der 35. Internationalen Konferenz über die Verankerung des Datenschutzes und des Schutzes der Privatsphäre im Völkerrecht;

Bezieht sich auf die laufenden Enthüllungen über die Existenz und Nutzung der elektronischen Massenüberwachungsprogramme seit dem Sommer 2013;

Ist sich bewusst, dass nicht alle Mitglieder der Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre die Zuständigkeit für Fragen bezüglich der staatlichen Überwachung haben;

Betont den grundlegenden Charakter des Rechts auf den Schutz der Privatsphäre und den Datenschutz;

Begrüßt und *bekräftigt* die Entschließung 68/167 der Generalversammlung der Vereinten Nationen, die zum Ausdruck brachte, dass die Rechte der Menschen aus dem Offline-Bereich auch online geschützt werden müssen, wozu auch das Recht auf den Schutz der Privatsphäre gehört;

Nimmt die Berichte des Privacy and Civil Liberties Oversight Boards der USA über Programme *zur Kenntnis*, die nach Paragraph 215 des USA Patriot Acts und unter Abschnitt 702 des USA Foreign Intelligence Surveillance Act betrieben werden;

In Kenntnis der Stellungnahme zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken der Artikel-29-Datenschutzgruppe;

Begrüßt mit großem Interesse den Untersuchungsbericht des Amtes der Hohen Kommissarin der Vereinten Nationen für Menschenrechte über "Das Recht auf Privatsphäre im digitalen Zeitalter";

1. Bekräftigt ihre Bereitschaft zur Teilnahme an dem vorgesehenen Dialog aller Beteiligter, der sich mit den Herausforderungen für das Recht auf Privatheit und Datenschutz im Zusammenhang mit der modernen Kommunikationstechnologie befassen sollte;

2. Beauftragt das Exekutivkomitee, die Internationale Konferenz in diesem Dialog zu vertreten;

3. Ruft die Mitglieder der Internationalen Konferenz auf, bezüglich aller elektronischen Massenüberwachungsprogramme sich für die Einhaltung der allgemeinen Datenschutzgrundsätze, zumindest wie sie 2009 in den Standards von Madrid festgeschrieben wurden, des Internationalen Paktes über bürgerliche und politische Rechte, der Konvention 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dessen Zusatzprotokolls wie auch anderer internationaler Instrumente einzusetzen sowie an nationalen und internationalen Dialogen aller Beteiligter zu diesem Thema teilzunehmen.

4. Ruft die Mitglieder der Internationalen Konferenz auf, die Einhaltung dieser allgemeinen Grundsätze zum Datenschutz und zum Schutz der Privatsphäre im Hinblick auf jegliche elektronische Überwachungsprogramme sicherzustellen, wenn nötig, indem wirksamere Befugnisse angestrebt werden, um den Herausforderungen und Risiken der Überwachung zu begegnen.

5. Bittet ihre Mitglieder, alle Informationen über die Massenüberwachungsprogramme und über bewährte Methoden zur Aufsicht über derartige Programme dem Exekutivkomitee zur weiteren Verteilung an die Mitglieder und Beobachter der Internationalen Konferenz mitzuteilen.

Die amerikanische Handelskommission (FTC) enthält sich bei der Abstimmung über diese Entschließung, da sie sich auf Angelegenheiten außerhalb ihrer Zuständigkeit bezieht.

Anlage 43

36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 13. bis 16. Oktober 2014 in Balaclava, Mauritius

Erklärung von Mauritius zum Internet der Dinge

Das Internet der Dinge wird bleiben. Immer mehr Gegenstände sind mit dem Internet verbunden und in der Lage, miteinander zu kommunizieren, manchmal ohne dass die Nutzenden dies bemerken. Diese Gegenstände können unser Leben sehr viel einfacher machen. Zum Beispiel bei der Gesundheitsversorgung, beim Transport oder der Energieversorgung können die verbundenen Gegenstände die Art und Weise verändern, mit der wir etwas erledigen. Das Internet der Dinge kann allerdings auch intime Details über das Handeln und die Bewegungen der Eigentümer von Gegenständen mithilfe der in ihnen enthaltenen Sensoren offenbaren.

Selbstbestimmung ist ein unveräußerliches Recht aller Menschen. Die persönliche Entwicklung sollte nicht dadurch festgelegt werden, was Unternehmen und Regierungen über den Einzelnen wissen. Die Ausbreitung des Internets der Dinge vergrößert allerdings das Risiko, dass dies geschehen wird. Die versammelten Beauftragten für Datenschutz und Privatsphäre haben deshalb die Möglichkeiten des Internets der Dinge und seine Konsequenzen während der 36. Internationalen Datenschutzkonferenz diskutiert, die in Balaclava, Mauritius am 13. und 14. Oktober 2014 stattfand. Vier Redner, die sowohl den wirtschaftlichen Sektor als auch die Wissenschaft repräsentierten, stellten den Beauftragten die positiven Veränderungen wie auch die Risiken vor, die das Internet der Dinge in unser tägliches Leben bringen kann. Die Redner gaben außerdem einen Überblick darüber, was getan werden muss, um den weiteren Schutz unserer personenbezogenen Daten wie auch unseres Privatlebens sicherzustellen.

Die anschließende Diskussion führte zu den folgenden Empfehlungen:

- Die beim Internet der Dinge verwendeten Sensoren erzeugen Daten in hoher Quantität, Qualität und Sensitivität. Dies bedeutet, dass sehr viel weiterreichende und sensitivere Folgerungen gezogen werden können und die Herstellung eines Personenbezugs wahrscheinlicher ist als dessen Vermeidung. Angesichts der Tatsache, dass die Personenbeziehbarkeit und der Datenschutz im Zusammenhang mit „Big Data“ an sich schon eine große Herausforderung sind, ist es deutlich, dass große Datenmengen, die von Gegenständen im Internet der Dinge gewonnen werden, diese Herausforderungen um ein Vielfaches vergrößern. Deshalb sollten solche Daten als personenbezogen angesehen werden.

- Obwohl für viele Unternehmen das Geschäftsmodell noch unbekannt ist, liegt der Wert des Internets der Dinge eindeutig nicht nur in den Geräten selbst. Das finanzielle Interesse liegt in den neuen Diensten im Zusammenhang mit dem Internet der Dinge und in den Daten.

- Jeder, der heute lebt, wird erkennen, dass Konnektivität allgegenwärtig ist. Dies mag noch mehr der Fall sein für die junge und zukünftige Generationen,

die sich keine Welt ohne Vernetzung vorstellen können. Es sollte aber nicht allein ihre Aufgabe sein, ob ihre Daten geschützt werden oder nicht. Es ist eine gemeinsame Verantwortung aller Handelnden in der Gesellschaft, damit das Vertrauen in vernetzte Systeme aufrechterhalten werden kann. Dafür ist Transparenz von entscheidender Bedeutung: Wer Dienstleistungen im Internet der Dinge anbietet, sollte klar sagen, welche Daten er sammelt, für welche Zwecke und wie lange diese Daten gespeichert werden. Er sollte Überraschungen für Verbraucher ausschließen. Beim Kauf von Gegenständen des Internets der Dinge oder entsprechender Programme sollte eine angemessene ausreichende und verständliche Information zur Verfügung stehen. Gegenwärtige Datenschutzerklärungen vermitteln nicht immer die Information in einer klaren, verständlichen Weise. Einwilligungen, die auf der Basis solcher Datenschutzerklärungen erteilt werden, können kaum als informierte Einwilligungen angesehen werden. Unternehmen müssen ihre Herangehensweise grundlegend verändern, damit Datenschutzerklärungen nicht länger in erster Linie dem Zweck dienen, sie vor Klagen zu schützen.

- Die Datenverarbeitung beginnt in dem Moment der Datenerhebung. Alle Schutzmaßnahmen sollten ab diesem Zeitpunkt greifen. Wir ermutigen zur Entwicklung von Technologien, die neue Wege der Einbeziehung von Datenschutz und Verbraucherschutz von Anfang an ermöglichen. „Privacy by Design and Default“ sollte nicht länger als etwas Abseitiges betrachtet werden. Beide Prinzipien sollten ein wesentliches Verkaufsargument für innovative Technologien werden.

- Das Internet der Dinge wirft auch wesentliche Sicherheitsrisiken auf, die beherrscht werden müssen. Eine einfache Firewall reicht längst nicht mehr aus. Ein Weg, um das Risiko für Betroffene zu begrenzen, liegt darin, dass man die Datenverarbeitung auf das Endgerät selbst beschränkt (lokale Verarbeitung). Wenn dies nicht möglich ist, sollten Unternehmen Ende-zu-Ende-Verschlüsselung vorsehen, um die Daten vor ungerechtfertigter Einwirkung oder Manipulation zu schützen.

- Die Datenschutz- und Privatsphäre-Behörden werden weiterhin die Entwicklungen beim Internet der Dinge beobachten. Sie machen es sich zur Aufgabe, die Befolgung der Datenschutzgesetze in ihren jeweiligen Ländern sicherzustellen, ebenso wie die Einhaltung der international akzeptierten Prinzipien. Wenn Rechtsverstöße festgestellt werden, werden sie angemessene Sanktionsmaßnahmen ergreifen, entweder einseitig oder durch internationale Zusammenarbeit.

- Angesichts der großen Herausforderungen, denen sich die Entwickler im Internet der Dinge, die Datenschutzbehörden und die Betroffenen gegenübersehen, sollten sich alle Beteiligten an einer starken, aktiven und konstruktiven Debatte zu den Konsequenzen des Internets der Dinge und der aus ihm gewonnen großen Datenmenge beteiligen, um das Bewusstsein für die zu treffenden Entscheidungen zu erhöhen.

Anlage 44

36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 13. bis 16. Oktober 2014 in Balaclava, Mauritius

Entschließung zu Big Data

– Übersetzung –

Es wird regelmäßig geltend gemacht, dass die Gesellschaft in mehrfacher Hinsicht von der Fähigkeit profitieren kann, riesige Mengen an Daten zu speichern und zu analysieren. So kann Big Data beispielsweise genutzt werden, um die Ausbreitung von Seuchen vorherzusagen, wichtige Nebenwirkungen von Arzneimitteln festzustellen und die Verschmutzung in Großstädten zu bekämpfen. Einige dieser Nutzungen kommen ohne personenbezogene Informationen aus; es gibt jedoch auch Nutzungen von Big Data, die wichtige Fragen in Bezug auf die Privatsphäre der Einzelnen und die Bürgerrechte sowie den Schutz vor Diskriminierung und Verstößen gegen das Recht auf Gleichbehandlung aufwerfen.

Bei Big Data kommt eine neue Einschätzung von Daten ins Spiel, wodurch Informationen erkennbar werden, die vorher nur schwer abzuleiten oder anderweitig verborgen waren. Big Data beinhaltet in großem Maße die Wiederverwendung von Daten. Der Wert der Daten hängt gewissermaßen davon ab, inwieweit sie Vorhersagen zu künftigem Handeln oder Ereignissen ermöglichen. Big Data kann als Infragestellung wesentlicher Datenschutzgrundsätze, insbesondere des Grundsatzes der Zweckbindung und der Datenvermeidung, wahrgenommen werden.

Der Schutz durch diese Datenschutzgrundsätze ist wichtiger als je zuvor, da immer mehr Informationen über uns gesammelt werden. Diese Grundsätze sind die Grundlage für Schutzmaßnahmen gegen eine extensive Profilbildung in immer weiteren, neuen Zusammenhängen. Wenn die wesentlichen Datenschutzgrundsätze verwässert werden und gleichzeitig extensiv von Big Data Gebrauch gemacht wird, wird sich das wahrscheinlich negativ auf den Datenschutz und andere Grundrechte auswirken.

Die Mitglieder der Internationalen Konferenz und andere Beteiligte, wie z. B. die International Working Group on Data Protection in Telecommunications (IWGDPT, auch bekannt als „Berlin Group“), haben sich mit Datenschutz und Fragen des Schutzes der Privatsphäre in Zusammenhang mit Big Data auseinandergesetzt. Mit Profilerstellungen und den damit einhergehenden Datenschutzfragen hat sich die Internationale Konferenz in der Uruguayer Erklärung von 2012 zur Profilbildung und in der Warschauer Erklärung zur Profilbildung von 2013 befasst. Um die Beteiligten weiter zu Anstrengungen zu ermuntern, mit denen die mit der Verwendung von Big Data verbundenen Risiken gesenkt werden sollen,

fordert die 36. Internationale Konferenz der Beauftragten für Datenschutz und die Privatsphäre alle Parteien, die Big Data verwenden, auf,

- den Grundsatz der Zweckbindung zu achten;
- das Ausmaß der Datenerhebung und -speicherung auf das für den beabsichtigten rechtmäßigen Zweck Erforderliche zu begrenzen;

- in Zusammenhang mit der Verwendung personenbezogener Daten für Analyse- und Profilerstellungszwecke gegebenenfalls eine gültige Zustimmung des Betroffenen einzuholen;

- transparent zu machen, welche Daten erhoben werden, wie die Daten verarbeitet, für welche Zwecke sie verwendet und ob sie an Dritte weitergegeben werden;

- den Einzelnen angemessenen Zugang zu den über sie erhobenen Daten und auch Zugang zu Informationen und sie betreffende Entscheidungen zu geben. Die Einzelnen sollten auch darüber informiert werden, aus welchen Quellen die verschiedenen personenbezogenen Daten stammen und gegebenenfalls das Recht haben, die über sie gespeicherten Angaben zu korrigieren und wirksame Instrumente zur Kontrolle der über sie gespeicherten Angaben zu erhalten;

- den Einzelnen gegebenenfalls Zugang zu Informationen darüber zu geben, welche wesentlichen Inputdaten und Entscheidungskriterien (Algorithmen) als Grundlage für die Erstellung des Profils genutzt wurden. Solche Informationen sollten in klarer und verständlicher Form vorgelegt werden;

- eine Datenschutzverträglichkeitsprüfung durchzuführen, insbesondere in Fällen, in denen die Analyse von Big Data mit neuen oder unerwarteten Formen der Nutzung personenbezogener Daten einhergeht;

- Big-Data-Technologien nach den Prinzipien von Privacy by Design zu entwickeln und anzuwenden;

- zu prüfen, in welchen Fällen die Verwendung anonymer Daten eine Verbesserung des Datenschutzes bewirkt. Eine Anonymisierung kann dazu beitragen, die datenschutzrechtlichen Risiken bei der Analyse von Big Data zu mindern. Das funktioniert aber nur, wenn die Anonymisierung technisch angemessen gestaltet und gehandhabt wird. Die optimale Lösung für die Anonymisierung von Daten sollte von Fall zu Fall festgelegt werden; dabei sollten möglicherweise mehrere Techniken miteinander kombiniert werden;

- vor der Weitergabe oder Veröffentlichung pseudonymisierter oder anderweitig indirekt identifizierbarer Datensätze große Sorgfalt walten zu lassen und das geltende Datenschutzrecht zu befolgen. Falls die Daten so detailliert sind, dass sie mit anderen Datensätzen verknüpft werden können oder personenbezogene Daten beinhalten, ist der Zugang zu beschränken und sorgfältig zu kontrollieren;

darzulegen, dass Entscheidungen rund um die Verwendung von Big Data fair, transparent und nachvollziehbar sind. Im Zusammenhang mit der Verwendung von Daten für die Zwecke der Profilerstellung bedürfen sowohl die Profile wie auch die zugrunde liegenden Algorithmen einer fortlaufenden Bewertung. Hierzu sind regelmäßige Kontrollen erforderlich um zu überprüfen, ob die Profilbildungsergebnisse verantwortbar, fair und ethisch vertretbar sind und ob die Vereinbarkeit und Verhältnismäßigkeit im Hinblick auf die Zwecke, für die die Profile verwendet werden, gewahrt ist. Unrecht gegenüber den Einzelnen aufgrund vollautomatischer falsch-positiver oder falsch-

negativer Ergebnisse sollte vermieden werden, und es sollte stets eine manuelle Bewertung von Ergebnissen, die von signifikanter Bedeutung für die Einzelnen sind, verfügbar sein.

Anlage 45

37. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre am 27. Oktober 2015 in Amsterdam

Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy

The 37th International Conference of Data Protection and Privacy Commissioners:

Noting that disastrous terrorist attacks and criminal activities increasingly lead to legislative measures disproportionally curtailing fundamental human rights such as the right to privacy;

Noting that the revelations of the massive electronic surveillance programmes have not yet led to legally binding instruments to regulate the intrusions into privacy by intelligence organisations on an international level;

Recalling the efforts being made on a global scale for international frameworks in support of data protection and privacy, including the resolution of the 35th Conference calling for the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[1];

Observing the increase of data being collected and processed by powerful international companies in a globalised economy;

Concerned about the potentially harmful consequences of such data gathering for the privacy rights of billions of individuals at the dawn of Big Data;

Detecting a pressing demand for regulating and enforcing data subjects' rights on a global scale adequately balancing states' and companies' desires against the human rights of individuals;

Referring to United Nation's General Assembly resolutions 68/167 of 18 December 2013[2] and 69/166 of 18 December 2014[3] on the Right to Privacy in the Digital Age which summarised the multiple challenges for privacy rights in a data driven world;

1. Welcomes the United Nation's Human Rights Council's resolution A/HRC/28/L.27 of 24 March 2015[4] which established a Special Rapporteur on

[1] http://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf

[2] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

[3] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166

[4] http://www.dgvn.de/fileadmin/user_upload/menschenr_durchsetzen/bilder/News/Menschenrechte_im_digitalen_Zeitalter/Resolution_2015_HRC_HR_in_the_digital_age-A_HRC_28_L27.doc

the Right to Privacy as a landmark decision towards internationalisation and globalisation of data protection and privacy rights;

2. Congratulates Professor Joseph Cannataci on his appointment as UN Special Rapporteur on the Right to Privacy;

3. Calls upon the UN Special Rapporteur on the Right to Privacy to include the cooperation with data protection and privacy authorities from around the world in his work programme;

4. Reaffirms the resolution of the 35th Conference on an additional protocol to Article 17 ICPPR and calls upon the UN Special Rapporteur on the Right to Privacy to promote the start of negotiations on such a protocol within his first mandate.

5. Calls upon governments and all relevant stakeholders to offer any assistance and support necessary to enable the UN Special Rapporteur in the best possible manner in order to promote and enhance privacy rights worldwide.

The U.S. Federal Trade Commission abstains from this resolution, which relates to matters outside its jurisdiction.

Weitere Dokumente

Anlage 46

Anhörung vor der Enquete-Kommission des Landtages von Sachsen-Anhalt zum Thema: „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“ vom 7. November 2014

Kernempfehlungen des Landesbeauftragten zum Schwerpunkt 3 des Einsetzungsbeschlusses „E-Government-Strategie“ unter den Gesichtspunkten des Datenschutzes und der Informationsfreiheit

(Entspricht der Vorlage 17, Ausschuss-Drs. 6/E07/7 vom 07.11.2014)

1. Das geplante Landesorganisationsgesetz, das eine E- und Open-Government-Regelung für die Landesverwaltung verlangt, sollte zügig verabschiedet werden.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014, Vortrag des Landesbeauftragten vor dem CDU Wirtschaftsrat am 11. September 2014.

2. Ein Landes-E-Government-Gesetz – als Ausdruck einer modernen Verwaltung – sollte noch in der sechsten Legislaturperiode verabschiedet werden.
   Bezug:
   Stellungnahme des Landesbeauftragten zur Anhörung am 19. April 2013 vor der Enquete-Kommission; Schreiben des Landesbeauftragten vom 20. Oktober 2014; Umsetzungsplan der Landesregierung zur IT-Strategie Sachsen-Anhalt digital 2020 vom 20. Mai 2014, Nr. 1.

3. Mit der Einführung der elektronischen Akte sollte zügig begonnen werden, denn sie ist eine Grundvoraussetzung für E- und Open-Government.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014; Umsetzungsplan der Landesregierung zur IT-Strategie Sachsen-Anhalt digital 2020 vom 20. Mai 2014, Nr. 14.

4. Mit dem Aufbau des von der Landesregierung im Masterplan Landesportal 2014-2016 beschlossenen Informationsregisters sollte planmäßig zum 1. Januar 2015 begonnen werden.
   a) Das Informationsregister ist als Kernprojekt in den Umsetzungsplan der „Strategie Sachsen-Anhalt digital 2020“ aufzunehmen.
   b) Das Informationsregister bedarf einer gesetzlichen Regelung.

   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014, vom 26. August 2014 sowie vom 2. Juli 2013 einschließlich Positionspapier und Entschließung der 26. Konferenz der Informationsfreiheitsbeauftragten zu Open Data vom 27. Juni 2013; Masterplan Landesportal 2014-2016; Aktionsplan der Bundesregierung zur Umsetzung der G8 Open-Data-Charta.

5. Sachsen-Anhalt braucht mit Blick auf die PSI-Richtlinie und das Informationsweiterverwendungsgesetz sowohl eine Open-Data- als auch eine Open-Government-Strategie. Die „Strategie Sachsen-Anhalt digital 2020“ ist im Bereich des E-Governments fortzuschreiben und um eine Open-Government-Strategie zu erweitern. Dazu ist die Strategie selbst und nicht nur der Umsetzungsplan anzupassen.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014 sowie vom 2. Juli 2013 einschließlich Positi-

onspapier und Entschließung der 26. Konferenz der Informationsfreiheitsbeauftragten zu Open Data vom 27. Juni 2013.

6. Die einzelnen IKT-Strategien der mittlerweile vier Dataport-Kern-Trägerländer sollten unter Einbeziehung des zentralen IT-Dienstleisters Dataport untereinander abgestimmt werden.
   Bezug:
   Vortrag des Landesbeauftragten vor dem CDU Wirtschaftsrat am 11. September 2014.

7. Die Zusammenarbeit mit dem Bund im Bereich von E- und Open-Government sollte hinsichtlich der Programme der Bundesregierung ausgebaut werden.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014; Digitale Agenda 2014-2017; Programm „Digitale Verwaltung 2020“ der Bundesregierung nebst den dazugehörigen Eckpunkten; Nationaler Aktionsplan zur Umsetzung der G8 Open-Data-Charta.

8. In diesem Zusammenhang sollte die Rahmenvereinbarung des Landes mit den kommunalen Spitzenverbänden zum E-Government um konkrete Maßnahmen ergänzt werden.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014; Digitale Agenda 2014-2017 sowie dem Programm „Digitale Verwaltung 2020“ der Bundesregierung nebst den dazugehörigen Eckpunkten.

9. Die verschlüsselte elektronische Kommunikation zwischen der Wirtschaft, den Bürgern und der Verwaltung, aber auch innerhalb der Verwaltung darf nicht aus finanziellen Gründen scheitern. Eine verpflichtende Regelung gehört ins Landes-E-Government-Gesetz.
   Bezug:
   Schreiben des Landesbeauftragten vom 20. Oktober 2014, Bundesgerichtshof, Beschluss vom 26. Februar 2013, Az. KVZ 57/12; vgl. auch Beschluss des Landtags „Vertrauliche Kommunikation fördern“, LT-Drs. 6/3532.

10. Die Einführung des elektronischen Rechtsverkehrs in der Justiz und der elektronische Rechtsverkehr in der Verwaltung des Landes müssen aufeinander abgestimmt werden.
    Bezug:
    Schreiben des Landesbeauftragten vom 20. Oktober 2014.

11. Die Landesleitlinie zur Informationssicherheit muss zügig verabschiedet werden. Sie bildet eine der Grundvoraussetzungen zum Anschluss des Landes Sachsen-Anhalt an das Verbindungsnetz ab dem 1. Januar 2015 gemäß § 3 des IT-NetzG.
    Bezug:
    Schreiben des Landesbeauftragten vom 20. Oktober 2014.

12. Der vollumfängliche Betrieb des neues Landesnetzes ITN-XT verzögert sich nach dem aktualisierten Umsetzungsplan der „Strategie Sachsen-Anhalt digital 2020“ von 2015 auf Ende 2017. Die Anforderungen des Datenschutzes und der Datensicherheit sollten im Vergabeverfahren Berücksichtigung finden.
    Bezug:
    Schreiben des Landesbeauftragten vom 20. Oktober 2014; Vortrag des Landesbeauftragten vor dem CDU Wirtschaftsrat am 11. September 2014; Umsetzungsplan der Landesregierung zur IT-Strategie Sachsen-Anhalt digital 2020 vom 20. Mai 2014, Nr. 3.

Anlage 47

Organigramm

SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Landesbeauftragter
Herr Dr. von Bose

Leitender Beamter der Geschäftsstelle und Stellvertreter
Herr Cohaus

Referat 1 Geschäftsstelle, Inneres, Justiz, Finanzen, Europa	**Referat 2** Landesdatenschutzgesetz, Soziales, Gesundheit, Bildung, Informationsfreiheit	**Referat 3** Informations- und Kommunikationstechnologie, E-Government, Medien	**Referat 4** Aufsichtsbehörde nach § 38 BDSG
Landtag, Justizverwaltung, Justizvollzug, Europäischer und Internationaler Datenschutz	Grundsatzfragen des Datenschutzrechts, Datenschutzmanagement Hochschulen, Kammern	Grundsatzfragen der Informationstechnik und der Organisation des Datenschutzes, E-Government, Verkehr	Düsseldorfer Kreis, Verbraucherdatenschutz, Datenschutzmanagement, Internationaler Datenverkehr
Polizei, Verfassungsschutz, Gefahrenabwehr	Informationszugangsrecht, Open Government	Telekommunikations- und Medienrecht, Presserecht, Verwaltungsmodernisierung	Gewerbe, Handel, Banken, Versicherungen, Bildungsträger, Wohnungswirtschaft
Finanzen, Kommunalrecht, Ausländerrecht	Sozialwesen, Verwaltungsverfahrensrecht	Technische Beratung nach BDSG, *IT der Geschäftsstelle*	Auftragsdatenverarbeitung, Adresshandel, Markt- und Meinungsforschung, Werbewirtschaft, Vereine, Videoüberwachung
Melde-, Pass- und Ausweiswesen, Personenstandwesen	Gesundheitswesen, Kinder- und Jugendhilfe, Wissenschaft und Forschung, Schulen, Archivwesen, Personalrecht	Betriebssysteme, Datenbanken, Netze, Verschlüsselung, IT-Grundschutz *IT der Geschäftsstelle*	
Geschäftsstelle: Haushalts- und Verwaltungsangelegenheiten		Vermessungswesen und Geoinformation, Statistik, Handwerk und Gewerbe *Internetauftritt des LfD*	
Geschäftsstelle: Vorzimmer des LfD, Schreibdienst, Bibliothek			
Geschäftsstelle: Registratur, Schreibdienst			
Geschäftsstelle: Registratur, Schreibdienst			
Geschäftsstelle: Kraftfahrer, Botendienst			

Stichwortverzeichnis

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z