SACHSEN-ANHALT

XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Dieser Text entspricht der Landtagsdrucksache 6/2602

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

Die digitale Durchdringung der Gesellschaft schreitet voran. Welchen Wert haben Privatheit, informationelle Selbstbestimmung und Datenschutz im digitalen Zeitalter? Dieses ist durch Globalität, Vernetzung, Virtualität bzw. Entkörperlichung sowie Entzeitlichung geprägt. Staatliche Schutzpflichten laufen der Entwicklung hinterher. Das gilt zumal für den rechtlichen Rahmen. Der Datenschutz durch Technik und der Selbstdatenschutz der Nutzer versagen oftmals angesichts moderner Überwachungssysteme. Der NSA-Ausspähskandal hat die Grundfragen nach dem Zustand der Grundrechte und von Demokratie und Rechtsstaat wieder neu aufgeworfen. Welche Datenschutzkultur – offenbar mit internationalen Maßstäben – benötigen wir? Freiheit und Vertrauen sollten, da sie Teil der rechtlichen und demokratischen Identität der Gesellschaft sind, erhalten und gestärkt werden. Dass dies auch Sachsen-Anhalt angeht, und wie dies im Datenschutzalltag, aber auch in der Rechtspolitik gelingen kann, darauf wird in diesem Bericht näher eingegangen.

Der XI. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2011 bis zum 31. März 2013. Bei einzelnen Beiträgen konnten noch darüber hinausreichende aktuelle Sachstände einbezogen werden (Redaktionsschluss: 1. Oktober 2013).

Prägend für die Tätigkeit der Geschäftsstelle im Berichtszeitraum war die Übernahme der Datenschutzaufsicht über den nicht-öffentlichen Bereich ab 1. Oktober 2011. Themen und Aufgaben sind auch dadurch weiter gewachsen.

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

Magdeburg, den 25. November 2013

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

Inhaltsverzeichnis

Anlagenverzeichnis

Nationale Datenschutzkonferenz

Abkürzungsverzeichnis

A	
AEG	Allgemeines Eisenbahngesetz
AOK	Allgemeine Ortskrankenkasse
App	Application (umgangssprachlich „kleines Programm“)
ArchG-LSA	Landesarchivgesetz
AZRG	Ausländerzentralregistergesetz
B	
bDSB	Behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BeiST	Projekt „Beitritt des Landes Sachsen-Anhalt zum IT-Trägerverbund der norddeutschen Länder“
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Medien e. V.
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung (Entscheidungssammlung)
BVerwG	Bundesverwaltungsgericht
BYOD	Bring Your Own Device („Bring dein eigenes Gerät mit“)
C	
CIO	Chief Information Officer (Leiter Informationstechnologie)
CNIL	Commission Nationale de l'Informatique et des Libertés
CoC	Code of Conduct
CR	Computer und Recht
D	
DG LSA	Disziplinargesetz Sachsen-Anhalt
DIN	Deutsches Institut für Normung e. V.
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
DuD	Datenschutz und Datensicherheit
DVDV	Deutsches Verwaltungsdiensteverzeichnis
E	
EBE	Erhöhtes Beförderungsentgelt
E-Geld	Elektronisches Geld
EGovG	E-Government-Gesetz des Bundes
eID	Elektronische Identität
EuGH	Europäischer Gerichtshof

F

FATCA	Foreign Account Tax Compliance Act

G

GBO	Grundbuchordnung
GCHQ	Government Communications Headquarters (Regierungskommunikationshauptquartier)
GDIG LSA	Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz für die Bundesrepublik Deutschland
GmbH	Gesellschaft mit beschränkter Haftung
GIW	Geoinformationswirtschaft
GKI Europol	Gemeinsame Kontrollinstanz Europol
GPS	Global Positioning System
GÜL	Gemeinsame elektronische Überwachungsstelle der Länder
GVBl. LSA	Gesetz- und Verordnungsblatt für das Land Sachsen-Anhalt
GWZ	Gebäude- und Wohnungszählung

H

HD	High Density
HSG	Hochschulgesetz des Landes Sachsen-Anhalt

I

IHK	Industrie- und Handelskammer
IHK-G	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
IHK-GfI	Industrie- und Handelskammer Gesellschaft für Informationsverarbeitung mit beschränkter Haftung
IKT	Informations- und Kommunikationstechnologie
INDECT	Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung
iOS	iPhone Operating System; Apple-Betriebssystem für Smartphones
IP-Adresse	Internetprotokoll-Adresse
IPTV	Internet Protocol Television, Internet-Fernsehen
IPv6	Internetprotokoll Version 6
ISO	International Organization for Standardization
IT	Informationstechnik
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
ITN-XT	zukünftiges Informationstechnisches Netz Sachsen-Anhalt – ITN-„eXTended“

IT-PLR	IT-Planungsrat
J	
JVA	Justizvollzugsanstalt
K	
Kfz	Kraftfahrzeug
KoSIT	Koordinierungsstelle für IT-Standards
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz)
L	
LBG LSA	Landesbeamtengesetz Sachsen-Anhalt
LfD	Landesbeauftragter für den Datenschutz
LHO	Landeshaushaltsordnung
LIR	Local Internet Registry, lokales IPv6-Register
LISA	Landesinstitut für Schulqualität und Lehrerbildung
LLIS	Landesleitstelle Informations-Strategie
LRZ	Landesrechenzentrum
LT-Drs.	Landtagsdrucksache
LTE	Long Term Evolution, Mobilfunkstandard 4. Generation
LVermGeo	Landesamt für Vermessung und Geoinformation Sachsen-Anhalt
M	
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MDK	Medizinischer Dienst der Krankenversicherung
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MMR	MultiMedia und Recht
MMS	Multimedia Messaging Service
MVZ	Medizinisches Versorgungszentrum
N	
NADA	Nationale Anti-Doping-Agentur
NADIS	Nachrichtendienstliches Informationssystem
NEGS	Nationale E-Government-Strategie
NFC	Near Field Communication (Nahfeldkommunikation)
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift – Rechtsprechungs-Report
nPA	neuer Personalausweis
NSA	National Security Agency (Nationale Sicherheitsbehörde)
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA-RR	Neue Zeitschrift für Arbeitsrecht, Rechtsprechungsreport
NZS	Neue Zeitschrift für Sozialrecht
O	
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
ÖPNV	Öffentlicher Personennahverkehr
ÖPNVG LSA	Gesetz über den öffentlichen Personennahverkehr im Land Sachsen-Anhalt

OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
OWiSch	Datenbank zur Erfassung von Ordnungswidrigkeiten im Bereich der Schwarzarbeit
P	
PassV	Verordnung zur Durchführung des Passgesetzes (Passverordnung)
PAuswG	Personalausweisgesetz
PC	Personalcomputer
PIA	Privacy Impact Assessment (Datenschutzfolgeabschätzung)
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PNR	Passenger Name Records
PPP	Public Private Partnership
PROMIS	Personal-, Ressourcen-, Organisationsmanagement- und Informationssystem für das Land Sachsen-Anhalt
PUK	Personal Unblocking Key
PVS	Personalvermittlungsstelle
R	
RDV	Recht der Datenverarbeitung
RettDG LSA	Rettungsdienstgesetz des Landes Sachsen-Anhalt
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
S	
SGB	Sozialgesetzbuch
SIS II	Schengener Informationssystem II
SMS	Short Message Service
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SSD	Solid State Drive
Steuer-ID	Steuer-Identifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
SÜG-LSA	Sicherheitsüberprüfungs- und Geheimschutzgesetz Sachsen-Anhalt
SVVollzG LSA	Sicherungsverwahrungsvollzugsgesetz des Landes Sachsen-Anhalt
T	
TFTP	Terrorist Finance Tracking Program
TFTS	Terrorist Finance Tracking System
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz

U

UAG	Unterarbeitsgruppe
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMTS	Universal Mobile Telecommunications System, Mobilfunkstandard 3. Generation
Unix	Mehrbenutzerbetriebssystem, Open Source
USA	United States of America (Vereinigte Staaten von Amerika)
USB	Universal Serial Bus
UWG	Gesetz gegen den unlauteren Wettbewerb

V

VEMAGS	Verfahrensmanagement für Großraum- und Schwertransporte
VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermGeoG LSA	Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt
VPN	Virtual Private Network (virtuelles privates Netz)
VRS	Verkehrsrechts-Sammlung

W

WADA	Welt-Anti-Doping-Agentur
WLAN	Wireless Local Area Network (lokales Funknetzwerk)
WP	Working Paper (Arbeitspapier)
WRV	Deutsche Verfassung vom 11. August 1919 – Weimarer Reichsverfassung

Z

ZD	Zeitschrift für Datenschutz
ZensAG LSA	Zensusausführungsgesetz Sachsen-Anhalt
ZensG 2011	Zensusgesetz 2011
ZPO	Zivilprozessordnung

1 Entwicklung und Situation des Datenschutzes

Social media, mobile computing, cloud computing, ubiquitous computing/ internet of everything – die Entwicklungen des Internets gehen ständig und nicht selten sprunghaft weiter. Jüngster Hype und Schwerpunkt ist BIG DATA.
Die Gefährdungen für die Grundrechte infolge der Überwachungspotentiale und ihrer Akteure und das Gefühl des Überwacht- und Kontrolliertwerdens wachsen ebenfalls sprunghaft.

Die Enquete-Kommission der 17. Legislaturperiode des Deutschen Bundestages „Internet und digitale Gesellschaft“ hat in ihren Bestandsaufnahmen die Situation zutreffend beschrieben. Doch die Handlungsempfehlungen bleiben eher mager.
Die von Mitgliedern des IT-Planungsrates initiierte Studie „Zukunftspfade Digitales Deutschland 2020“, die das E-Government als wesentlichen Nutzenstifter und Treiber hervorhebt, benennt u. a. folgende Pflichtbereiche staatlicher Aufgabe: Gewährleistung starker IT-Sicherheit und hohen Datenschutzes – Unterstützung digitaler Souveränität bzw. Medienkompetenz.

Doch müssten nicht vor allem die vielfältigen Überwachungen zurückgenommen werden? Wie sonst sollte Vertrauen als Voraussetzung einer gelingenden Digitalisierung entstehen und bestehen? Der NSA-Ausspähskandal hat diese Fragen erneut und in neuer Dimension aufgeworfen. Doch die Antworten bleiben weitgehend aus.
Bei möglichen Lösungsansätzen wird man die Herausforderung der Internationalisierung und gerade beim Verhältnis Europas zu den USA den Umstand unterschiedlicher Datenschutzkulturen zu berücksichtigen haben.

„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."

Der NSA-Ausspähskandal hat einige Träume beendet, den Traum von der absoluten Freiheit des Internets, von der Anonymität des Internets, den Traum von absoluter IT- und Datensicherheit im Internet. Propheten haben schon früher gewarnt, doch – aus den Träumen aufgewacht – erlebt man den realen Albtraum der Schaffung absoluter Sicherheit.
Dies geht hinein bis in die Gedankenfreiheit des Menschen, die auch der Bundesgerichtshof noch zum menschenwürdegeschützten Persönlichkeitskern zählt (Urteil vom 22. Dezember 2011, NJW 2012, 945).
Doch der Mensch wird zur Sache, algorithmengesteuerte Verfahren und prädiktive Analysen bestimmen das Verhalten vor. Ein Innenraum freier Selbstbestimmung (vgl. BVerfGE 27, 1, 6-7) verkommt zur Hülse. Das Gemeinwohl der demokratischen Gesellschaft leidet angesichts der Überwachungssysteme mit.

Das geht auch Sachsen-Anhalt an. Der öffentliche Diskurs zu diesen Zukunftsfragen ist allerdings verhalten. Auch wenn Sachsen-Anhalt scheinbar eine NSA- und GCHQ-freie Zone ist (vgl. LT-Drs. 6/2384 und 6/2455), gehören die Themen auf die öffentliche Tagesordnung. Denn auch hier klaffen Anspruch und Realität des Datenschutzes auseinander, was an folgenden Widersprüchen deutlich wird:

Die meisten Internetnutzer haben angeblich – bei freundlichem Desinteresse am Datenschutz – nichts zu verbergen. Die Wirtschaft und die Machtmonopole des Internets beanspruchen die Datenprofile für sich. Der Staat verweist auf die Datenmissbräuche dieser Akteure, fordert vom überforderten einzelnen Menschen mehr Selbstdatenschutz, um zugleich als Präventionsstaat zugunsten von totaler Sicherheit selbst Big Data zu betreiben, und dann scheinfreundlich den Bürger zur Nutzung von Angeboten des E-Government zu animieren – o tempora, o mores.

Der in schwerer Zeit entstandene XI. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2011 bis 31. März 2013; darüber hinausreichende Entwicklungen bis in den Herbst 2013 wurden mitberücksichtigt.

Der Bericht knüpft an den X. Tätigkeitsbericht (LT-Drs. 6/398) an und berücksichtigt auch die Entschließung des Landtages vom 19. Oktober 2012 (LT-Drs. 6/1545) und die dazugehörige Stellungnahme der Landesregierung (LT-Drs. 6/1733).

Für den Datenschutz im nicht-öffentlichen Bereich wird an den Fünften Tätigkeitsbericht des Landesverwaltungsamtes (01. Juni 2009 bis 30. September 2011) angeknüpft.

Inhaltlich geht es auch im aktuellen Bericht um Konzeptionen und Maßnahmen des Datenschutzes in den vier (oben bereits genannten) Bereichen **Recht, Technik, Kontrolle und Medienkompetenz** (diese Elemente werden auch von der Landesregierung in ihrer Stellungnahme zum X. Bericht bestätigt, LT-Drs. 6/997).

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.

Der Bericht greift wiederum datenschutzpolitische Themen auf; dazu wird auch auf die im Anlagenteil aufgenommenen Entschließungen verwiesen.

Der Bericht behandelt rechtliche und technische Entwicklungen und stellt Materialien und praxisbezogene Hinweise aus ausgewählten anschaulichen Einzelfällen, Beratungen und Kontrollen zur Verfügung.

1.1 Sicherheit und Freiheit

Zum Spannungsfeld von Sicherheit und Freiheit, in welchem sich der Datenschutz bewegt, hat sich der Landesbeauftragte wiederholt und unter Würdigung unterschiedlicher Aspekte geäußert. Insbesondere soll hier auf die Ausführungen im VIII. Tätigkeitsbericht zum Primat der Freiheit (Nr. 1.1), im IX. Tätigkeitsbericht zum Abwehrcharakter der Grundrechte (Nr. 1.1) und im X. Tätigkeitsbericht zur Überwachungs-Gesamtrechnung (Nr. 1.1) verwiesen werden.

Die Balance zwischen Sicherheit und Freiheit ist durch vielfältige elektronisch unterstützte staatliche Datenerhebungen und -verarbeitungen ständig in Gefahr, und das Gewicht verschiebt sich weiter in Richtung Sicherheit bis hin zu einem „Supergrundrecht“ auf Sicherheit. Der Präventionsstaat sammelt auf Vorrat, anlasslos, jedermann erfassend, im Vorfeld von Gefährdungen. Typisches Beispiel für entsprechende Vorstöße sind die wiederkehrenden Forderungen nach einer Ausweitung von Videoüberwachungen, so auch in Sachsen-Anhalt, bis hin zu heimlichen großflächigen Überwachungen, obwohl das die Polizeigesetze und zumal die Verfassungen nicht erlauben. Der „demokratische Überwachungsstaat“ wahrt nicht mehr das Maß und schränkt die Freiheitsrechte verfassungswidrig ein. Das gilt auch und insbesondere für das Tätigwerden seiner Nachrichtendienste. Doch es gibt – auch nicht infolge der Ausspähungen ausländischer Dienste – keine absolute Sicherheit.

Auf Landesebene wie auf Bundes- und europäischer Ebene gilt es, Balance zu halten und die Freiheitsrechte zu wahren. Rechtsstaat und Demokratie verdienen diesen Freiheitsgedanken, denn ohne ihn, konkret ohne informationelle Selbstbestimmung, leidet das Fundament, das die Gesellschaft trägt.

Die Datenschutzbeauftragten des Bundes und der Länder haben aktuelle Forderungen an Legislative und Exekutive gestellt:

„Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./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 Datenauswer-

tung 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' 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 Datenverarbeitung 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."

1.2 Nicht-öffentlicher Bereich

Der Schutz der Verbraucher bezieht sich nicht nur auf finanzielle Aspekte (vgl. dazu das Gesetz gegen unseriöse Geschäftspraktiken vom 1. Oktober 2013, BGBl. I S. 3714). Mit der zunehmenden Digitalisierung ist auch der **Schutz des Persönlichkeitsrechts der Verbraucher** in den Vorder-

grund geraten. Die Daten der Verbraucher, wie z. B. ihr Konsumverhalten oder die aktuellen Adressdaten, sind selbst zum Wirtschaftsgut geworden. Deshalb hat der Landesbeauftragte seit langem dafür geworben, sich verstärkt in der Schaffung des notwendigen Bewusstseins und der gebotenen Transparenz bei den Unternehmen und der Aufklärung der Verbraucher über ihre Rechte zu engagieren. Die Unternehmen müssen Datenschutz als Führungsaufgabe verstehen und im Rahmen eines strukturierten Datenschutzmanagements die Sicherheit und angemessene Verwendung der oft sensiblen Informationen ihrer Kunden gewährleisten (siehe auch Nr. 4.6). Die Bürgerinnen und Bürger müssen ihre Rechte kennen, um das Persönlichkeitsrecht selbstbestimmt wahrnehmen zu können. Das Ziel verlangt Zusammenarbeit der für die Förderung verantwortlichen Stellen im Land und die Schaffung einheitlicher Ansprechpartner.

Der Landtag von Sachsen-Anhalt hat sich mit Beschluss vom 19. Oktober 2012 (Drs. 6/1545) den Forderungen angeschlossen und stärkere Impulse und Kooperationen gefordert. Gemäß der Bitte des Landtags hat die Landesregierung den Landesbeauftragten zur Teilnahme an Beratungen einer interministeriellen Arbeitsgruppe zum Verbraucherschutz (federführend zuständig ist das Ministerium für Arbeit und Soziales) eingeladen. In diesem Rahmen regte der Landesbeauftragte an, sich an auf Bundesebene bestehenden Portalen wie z. B. „Verbraucher sicher online“ oder „Surfer haben Rechte“ zu orientieren. Durch Verlinkungen aus dem Landesportal könnte zur Information und zur Befähigung zum Selbstschutz beigetragen werden. Weitere Maßnahmen müssten auf den Teil der Bevölkerung zielen, der das Medium Internet nicht nutzt. In der Arbeitsgruppe wurden weitere Entwicklungsbereiche betrachtet, wie beispielsweise die Gebiete des Schulwesens, der Schulsozialarbeit und der kulturellen und politischen Bildung. Der Landesbeauftragte betonte den Zusammenhang von Medienkompetenz und Datenschutz (vgl. Nr. 9.5). Er bot den Ressorts seine Mitwirkung an Veranstaltungen und Projekten zum Verbraucherschutz/Verbraucherdatenschutz an.

Neben Datenschutzmanagement und Verbraucherbildung geht es natürlich weiterhin um ein modernes Datenschutzrecht (national wie international), das die Gefährdung für die Grundrechte infolge der technischen Entwicklungen in der digitalen Welt abwehrt (vgl. X. Tätigkeitsbericht, Nr. 1.2). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dient auch dem Verbraucherschutz, und das nicht nur bei Big Data (vgl. Nr. 1.3), und bedingt einen geregelten Datenschutz durch Technik. Strukturellen Risiken durch Profilbildungen ist z. B. durch Anonymisierungen zu begegnen (so auch der Bundestag in seinem Beschluss vom 13. Juni 2013 zu Nr. 2 der BT-Drs. 17/13936).

Ein gewisses rechtliches Neuland besteht noch bei der wettbewerbsrechtlichen Abmahnfähigkeit von Datenschutzverstößen. So hat z. B. das OLG Karlsruhe die Anwendung von §§ 4 Abs. 1, 28 BDSG als Marktverhaltensregeln im Sinne des § 4 Abs. 1 Nr. 11 des Gesetzes gegen den unlauteren Wettbewerb bejaht (Urteil vom 9. Mai 2012, NJW 2012, 3312; es ging um Werbeschreiben eines Energieversorgers an frühere Kunden in Kenntnis des Wechsels zum neuen Stromlieferanten). Dagegen hat etwa das OLG

München festgestellt, dass Datenschutzvorschriften nur den einzelnen Kunden schützen, nicht aber das Marktverhalten von Unternehmen mitregeln (Urteil vom 12. Januar 2012, RDV 2012, 149).

1.3 Informations- und Kommunikationstechnologie – Big Data

Immer mehr Daten lassen sich zu immer geringeren Kosten erheben und für eine eventuelle spätere Nutzung speichern, sei es im privaten Umfeld, sei es durch Unternehmen oder Behörden. Big Data ist Synonym für die riesigen Datensammlungen, in denen das „Wissen“ aus dem frei zugänglichen Internet, von Archiven, Unternehmen, Behörden, Kommunen und Privatpersonen gespeichert wird. Mittels Big Data werden Methoden, Technologien, IT-Architekturen und Auswertungssoftware zur Verfügung gestellt, um diese exponentiell steigenden Datenvolumen für quantitative und qualitative Analysen und somit für strategische Entscheidungsfindung zugänglich zu machen. Alle zwei Jahre verdoppelt sich das Volumen der gespeicherten Daten weltweit. Ein Ende des Wachstums dieser riesigen Datenmengen, welche aus dem Internet oder auch anderweitig gesammelt, verfügbar gemacht und entsprechend ausgewertet werden, ist nicht absehbar, denn die Speicherung von Daten ist schon lange kein relevanter Kostenfaktor mehr. Diese riesigen Datenmengen, oft sogar unstrukturiert, werden in der digitalen Welt immer mehr zu einem Produktionsfaktor neben Kapital, Arbeitskraft und Rohstoffen. Bestimmte Bereiche in den Unternehmen der Wirtschaft, wie u. a. Forschung und Entwicklung, Marketing, Produktion und Vertrieb, sind geradezu prädestiniert für den Einsatz von Big Data. Mittels Cloud Computing werden der Austausch und das Anlegen solcher riesigen Datensammlungen wesentlich erleichtert. Zudem stellen auch Verwaltungen im Rahmen von Open Government oder Open Data immer mehr Daten im Internet jedermann zur Verfügung (vgl. den Leitfaden des BITKOM von 2012).

Diese riesigen Datenmengen bieten ein enormes Potential für neue ökonomische, gesellschaftliche, wissenschaftliche und soziale Erkenntnisse. Forscher können neues Wissen ableiten, Unternehmen ihre Marktpositionierung verbessern, private Haushalte erlangen Komfortgewinn und können sparsamer mit Ressourcen umgehen, neue Produkte mit neuen Eigenschaften entstehen. Der Staat findet Hinweise auf terroristische Planungen oder zur Aufklärung von Verbrechen und bedient sich dabei Public-Private-Partnerships von Sicherheitsbehörden und Unternehmen. Doch auch die Risiken durch diese moderne Form der Rasterfahndung sind enorm. Daten werden in alle Richtungen verknüpft, neue Daten entstehen, informationeller Machtmissbrauch wird möglich, Grund- und Menschenrechte können massiv verletzt werden. Aus diesem Grund darf die Nutzung von Big Data-Ressourcen nur nach einer Risiko- und Technikfolgenabschätzung unter Einbeziehung von Politik, Gesellschaft, Wissenschaft und Datenschutzbeauftragten erfolgen.

Letztlich wird Big Data dort genutzt werden, wo sich Geld beschaffen oder einsparen lässt: Direkt beim Kunden. Beschrieben wird dieser Vorgang auch durch den Begriff „Consumerization“: Die meisten neuen Technolo-

gien – vor allem aus dem IT-Bereich – setzen sich zuerst beim Verbraucher durch und breiten sich erst später weiter in Unternehmen und Behörden aus.

Relationale Datenbanksysteme klassischer Art haben zunehmend massive Probleme, derart große und unstrukturierte Daten effektiv zu verarbeiten und zu visualisieren. Aus diesem Grund wird massiv parallel rechnende Spezialsoftware entwickelt und verwendet, welche diese Daten analysiert und so neue Informationen sowie neue Erkenntnisse daraus generieren soll.

Insbesondere die im Jahr 2013 bekannt gewordenen umfangreichen Spionage- und Überwachungsprogramme amerikanischer und britischer Geheimdienste bereiten den Bürgerinnen und Bürgern zunehmend Sorgen und schüren die Ängste vor Big Data. Programme wie PRISM und XKeyScore tragen Daten zu Einzelpersonen aus verschiedensten Quellen zusammen und erlauben die umfassende Überwachung ihrer Kommunikation durch aktive Zuarbeit der beteiligten Diensteanbieter, teilweise sogar in Echtzeit. Das britische Programm Tempora ist der Codename des dortigen Geheimdienstes Government Communications Headquarters (GCHQ) für ein ähnliches Projekt. Es dient auch der Überwachung des weltweiten Datenverkehrs in Telekommunikations- und Internet-Netzwerken.

Der Landesbeauftragte empfiehlt den sachsen-anhaltischen Behörden, Unternehmen und Kommunen, ihre Datenschutz- und Datensicherheitskonzepte zu überprüfen, ob diese allen aktuell vorstellbaren Gefährdungsszenarien standhalten. Insbesondere wenn öffentliche Stellen mit privaten Anbietern zusammenarbeiten, welche durch ihre Cloud-Angebote oder auch E-Mail- oder Internet-Dienstleistungen vermutlich mit ausländischen Geheimdiensten kooperieren (müssen) oder im Fokus dieser stehen, ist dringend zu prüfen, ob dies noch den Forderungen des DSG LSA bzw. BDSG entspricht.

Der Landesbeauftragte fordert beim Thema Big Data öffentliche Stellen wie Unternehmen auf, den Datenschutz und bestimmte Grundsätze zu beachten:

- Bei Big Data-Lösungen muss der Datenschutz oberste Priorität besitzen. Die Datenverarbeitung darf nur auf gesetzlicher Grundlage bzw. nur mit Einwilligung der Betroffenen erfolgen.

- Nur transparente Big Data-Lösungen (Algorithmen wie Datenbestände) ermöglichen Öffentlichkeit und erlauben Nutzern, Betroffenen, Politikern, Datenschutzbeauftragten und interessierten Dritten, sich Wissen und einen Überblick zur Entwicklung bei Big Data zu verschaffen. Ohne Transparenz auch bereits in der Planungsphase sind entstehende Gefahren nicht erkennbar.

- Die Verarbeitung von Daten muss grundsätzlich in anonymisierter Form erfolgen, damit eine Rückführung auf einzelne Personen nicht möglich ist. Der Einsatz von Techniken zum Erhalt der Privatsphäre,

wie eine wirksame quellennahe Anonymisierung der Datenströme, ist Pflicht. Eine mögliche Deanonymisierung der Daten einzelner Personen durch Zusammenführung verschiedener anonymisierter Datenbestände muss durch eine sofort anschließende erneute Anonymisierung ausgeschlossen werden.

Big Data-Erkenntnisse dürfen nur erfasst, ausgewertet und insbesondere veröffentlicht werden, wenn dadurch betroffene Einzelpersonen oder Gruppen nicht diskriminiert werden können. Ergebnis-Daten, die Rückschlüsse auf einzelne Personen erlauben, dürfen nicht veröffentlicht werden.

1.4 Zusammenfassung und Ausblick

Bald 30 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 16. Dezember 1983 (BVerfGE 65, 1) ist es dringend notwendig, dessen Maßstäbe in Erinnerung zu rufen und neu zu bekräftigen, zu beherzigen und umzusetzen. Rechtsstaatlichkeit, Grundrechtsschutz und Demokratie benötigen mehr Beachtung: Informationelle Selbstbestimmung als Teil des Persönlichkeitsrechts ist Funktionsbedingung der freiheitlichen Demokratie. Datenschutz ist Freiheitsmaßstab der Gesellschaft.

Datenschutz ist zugleich Vertrauensfaktor, doch dieser hat weiter gelitten, weil der Staat bei seinem eigenen Datengebaren oftmals die Grundrechte missachtet und zudem seinen Schutzverpflichtungen gegenüber dem Datengebaren der Wirtschaft nicht hinreichend nachkommt. Es ist höchste Zeit für vertrauensbildende Maßnahmen, um verloren gegangenes Vertrauen zurückzugewinnen.

Der Schutzauftrag aus den Grundrechten bei Privatrechtsverhältnissen im Sinne einer mittelbaren Grundrechtswirkung kann insbesondere bei großen Internetunternehmen und anderen Machtmonopolen sogar so weit gehen wie bei der unmittelbaren Grundrechtswirkung (so das Bundesverfassungsgericht in seiner Fraport-Entscheidung, NJW 2011, 1201).

Situation und Zukunft des Datenschutzes und entsprechende aktuelle politische Forderungen werden in einer Positionierung der Datenschutzkonferenz zusammengefasst:

„Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./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 Bun-

destages 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.*

- *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.*

- *Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.“

(Die vorgenannten Spiegelpunkte sind durch weitere Entschließungen konkretisiert worden. Siehe zum ersten Spiegelpunkt die unter Nr. 1 und Nr. 1.1 aufgenommenen Texte. Siehe zum zweiten und dritten Spiegelpunkt die Entschließungstexte zum Sozial- und Gesundheitswesen und zur Ende-zu-Ende-Verschlüsselung durch OSCI-Transport auf der Homepage des Landesbeauftragten.)

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die **Geschäftseingänge** entwickelten sich wie folgt:

2007: 3350 2008: 3730 2009: 4045 2010: 4109

2011: 4101 2012: 4710

Insgesamt wurden in 2011/2012 ca. 3.200 schriftliche Äußerungen verfasst (2009/2010: 2950; 2007/2008: 2300).

Im Zeitraum 2009/2010 gab es insgesamt 138 Petenteneingaben im Bereich des Datenschutzes bei öffentlichen Stellen. Im Zeitraum 2011/2012 erhöhte sich die Anzahl der Eingaben auf 169.

Für den nicht-öffentlichen Bereich ist der Landesbeauftragte seit dem 1. Oktober 2011 zuständig (siehe Nr. 3.1.4). Die Geschäftszahlen stellen sich wie folgt dar:

Beim Landesverwaltungsamt fielen im Zeitraum 2008 bis September 2011 646 Fälle an, davon wurden dem Landesbeauftragten am 1. Oktober 2011 unerledigte 161 Fälle übergeben. Von den Altfällen des Landesverwaltungsamtes waren bis Mitte 2013 noch 35 Fälle nicht abgeschlossen.

Insgesamt fielen in 2011 beim Landesverwaltungsamt und beim Landesbeauftragten 167 Fälle (davon beim Landesbeauftragten 38) an, in 2012 (nur beim Landesbeauftragten) 121 Fälle, bis Mitte 2013 47 Fälle. Bei der Bewertung des Rückgangs der Eingaben ist zu beachten, dass in den Angaben des Landesverwaltungsamtes auch Weiterleitungen wegen Unzuständigkeit der Behörde erfasst wurden; dies erfolgt beim Landesbeauftragten nicht in dieser Weise. Schwerpunkte ergeben sich in den Bereichen Videoüberwachung (vgl. Nr. 4.17), Beschäftigtendatenschutz und allgemein beim Kundendatenschutz.

Kontrollen wurden anlassabhängig und anlassunabhängig durchgeführt: Besondere Aufmerksamkeit erhielten die Kontrollen zu den Erhebungsstellen Zensus 2011 und die Kontrolle zum Maßregelvollzug im Landeskrankenhaus Uchtspringe. Weitere Prüfungsschwerpunkte waren die Überprüfungen in kommunalen Bereichen. Vier Kommunen wurden im Rahmen von Querschnittsprüfungen kontrolliert. Die Ratsinformationssysteme zweier Städte sowie mehrere Einwohnermeldeämter, Personalausweisbehörden, zwei Gesundheitsämter, eine Ausländerbehörde und ein Personalamt wurden im Berichtszeitraum ebenfalls überprüft. Des Weiteren wurden Vorgänge mit datenschutzrechtlicher Aktualität bei einigen kommunalen Schiedsstellen begutachtet. Zwei berufsbildende Schulen, zwei Gymnasien und das Landesschulamt standen auch im Fokus einer Prüfung. Kontrolliert wurde weiterhin ein Finanzamt, das eTicketing in Halle, ein Klinikum und die Sicherheitsakten im Geheimschutz in zwei Ministerien.

Nach der Übernahme der Zuständigkeit für den Datenschutz im nichtöffentlichen Bereich fanden auch hier vermehrt Kontrollbesuche statt. Der Schwerpunkt lag dabei auf der Überprüfung von Anlagen zur Videoüberwachung. Dies betraf sowohl Anlagen bei Unternehmen als auch bei Privatpersonen in Halle und in Magdeburg.

Informationsbesuche erfolgten u. a. zum Datenschutzkonzept im Landeskrebsregister und zur Umsetzung der europäischen Dienstleistungsrichtlinie sowie zur Datei NADIS (neu) beim Bundesamt für Verfassungsschutz. Regelmäßige Beratungsgespräche zum Sozialdatenschutz finden mit der AOK und dem MDK statt. Weitere Informationsbesuche fanden zu datenschutzrechtlichen Fragen der Qualitätssicherung im Landesportal statt.

Der Öffentlichkeitsarbeit wurde weiterhin besonderes Augenmerk geschenkt, mittels ständiger Aktualisierung des Angebots auf der Homepage, Pressemitteilungen, Interviews und Hinweisen.

Durch den Landesbeauftragten und Mitarbeiter der Geschäftsstelle wurden im Berichtszeitraum Vorträge gehalten und Fortbildungen durchgeführt.

Netzwerke

Seit einiger Zeit führte der Landesbeauftragte Gespräche mit dem Ziel, ein gemeinsames Treffen mit den behördlichen Datenschutzbeauftragten der Hochschulen zu organisieren. Dank des Engagements einzelner Hochschulen und ihrer Datenschutzbeauftragten kam im Berichtszeitraum nun ein Erfahrungsaustausch zustande. Aktuelle datenschutzrechtliche Themen und hochschulspezifische Problemstellungen wurden angesprochen. Im Ergebnis wurde zur Aufrechterhaltung des Erfahrungsaustauschs und zur Verbesserung der Kommunikation eine Mailingliste durch einen Hochschuldatenschutzbeauftragten eingerichtet.

Auch der regelmäßige Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der Landkreise wurde im Berichtszeitraum fortgesetzt. Hierbei konnte der Landesbeauftragte über aktuelle Themen und Entwicklungen berichten und über datenschutzrechtliche Rahmenbedingungen zu häufigen Fragestellungen, wie z. B. zum Inkasso kommunaler Forderungen, zu Ratsinformationssystemen oder technischen Aspekten, informieren.

Nach Übertragung der zusätzlichen Aufgabe der Aufsicht über den nichtöffentlichen Bereich wurde in Zusammenarbeit mit den Industrie- und Handelskammern des Landes und dem Bundesverband mittelständische Wirtschaft (BVMW) begonnen, ein Netzwerk zum Informations- und Erfahrungsaustausch aufzubauen, aus dem heraus Informationsveranstaltungen durchgeführt werden. Der Landesbeauftragte beteiligt sich an dem Erfahrungsaustauschkreis Sachsen-Anhalt der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) für betriebliche Datenschutzbeauftragte.

Gleichzeitig war es eine große Herausforderung, die personelle und sächliche Mehrausstattung in der Geschäftsstelle umzusetzen. Die personelle Besetzung in dem neuen Referat „Aufsichtsbehörde nach § 38 BDSG“ konnte im Juli 2013 abgeschlossen werden.

Das aktuelle Organigramm der Geschäftsstelle ist beigefügt (**Anlage 45**).

Am 19. April 2012 fand auf Einladung des Landesbeauftragten eine Vortragsveranstaltung aus Anlass des vor 20 Jahren (genau am 1. April 1992) in Kraft getretenen ersten Datenschutzgesetzes des Landes Sachsen-Anhalt statt. In einem Rückblick wurde auf die Hintergründe der Datenschutzbestimmungen im Gesetz sowie in der Landesverfassung und vor allem auf die aktuellen Entwicklungen in Folge des Internets eingegangen. Den Festvortrag hielt der Richter des Bundesverfassungsgerichts Prof. Dr. Johannes Masing (siehe NJW 2012, 2305).

2.2 Schwerpunkte – Empfehlungen

Wichtige Einzelvorgänge im Berichtszeitraum betrafen:

- PPP-Projekt Justizvollzugsanstalt Burg (Nr. 7.3)
- Verfassungsschutz – Moratorium bei Aktenvernichtung (Nr. 8.2)
- Soziale Netzwerke – Nutzung durch öffentliche Stellen (Nr. 4.19.1)
- Eingaben im Bereich Videoüberwachungen (Nr. 4.17)
- Landeskrebsregister (Nr. 10.1.4)
- Herzinfarktregister (Nr. 10.1.5)

Längerfristige Vorgänge betreffen:

- Modernisierung des Datenschutzrechts auf europäischer, Bundes- und Landesebene (Nr. 3.1)
- Reform der Sicherheitsbehörden (Nrn. 5.3 und 8.1)
- Datenschutzmanagement (Nr. 4.6)
- Informations- und Kommunikationstechnologie – Big Data (Nr. 1.3)
- IKT-Strategie i. V. m. E-Government-Vorhaben (Nr. 4.2)
- IT-Dienstleister Dataport (Nr. 4.4)
- Krankenhausinformationssysteme (Nr. 10.1.1)
- Forschungsprojekte (Nr. 9.1)

Mitwirkung an besonderen Gesetzgebungsverfahren:

- DSG LSA 2011 (Nr. 3.1.4)
- SOG LSA (Nr. 5.1)
- Bundesmeldegesetz (Nr. 5.9.1)
- Sicherungsverwahrungsvollzugsgesetz (Nr. 7.4)
- Schulgesetz (Nr. 9.4)
- Rettungsdienstgesetz (Nr. 10.1.12)

Der Landesbeauftragte äußert – ungeachtet der Empfehlungen und Maßgaben in den Einzelbeiträgen – die folgenden Grunderwartungen.

Empfehlungen und Forderungen an Landesregierung und Landtag:

- Modernisierung des DSG LSA (Nr. 3.1.5)
- Stärkung des Verbraucherdatenschutzes (Nr. 1.2)
- Intensivierung der Umsetzung des Konzepts zur Medienkompetenzbildung (Nr. 9.5)
- Schaffung eines E-Government-Gesetzes LSA (Nr. 4.2)
- Grundrechtskonforme Reform der Sicherheitsbehörden (Nrn. 5.3, 8.1); Beachtung des Trennungsgebotes
- Überwachungs-Gesamtrechnung vor neuen Überwachungssystemen und -maßnahmen
- Evaluierung vorhandener Überwachungen unter Einbeziehung der technischen Entwicklungen und Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- Evaluierung des SOG LSA und des VerfSchG-LSA; Befristung von Datenbefugnissen

2.3 Zusammenarbeit mit anderen Institutionen

Mit dem **Landtag**, insbesondere seinen Ausschüssen, bestanden vielfache Kontakte, insbesondere infolge von Beratungsaufgaben bei Gesetzgebungsvorhaben. Bemerkenswert ist die Entschließung zum X. Tätigkeitsbericht (LT-Drs. 6/1545), der in fast allen Landtagsausschüssen beraten worden war.

Auch mit den Fraktionen gab es vielfache Kontakte.

Ebenso wurde die vertrauensvolle Zusammenarbeit mit dem **Landtagspräsidenten und der Landtagsverwaltung** weiter gepflegt.

Verantwortliche Stellen der **Exekutive** wie Ministerien, Behörden etc. und private Verbände, Unternehmen etc. fragen weiter die Beratung durch den Landesbeauftragten nach.

Die Zusammenarbeit mit den Kolleginnen und Kollegen auf der Ebene der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** und ihren Arbeitskreisen und Arbeitsgruppen (vgl. zum Düsseldorfer Kreis Nrn. 13.1 und 13.1.1) ist intensiv und fruchtbar.

3 Nationales und internationales Datenschutzrecht

3.1 Novellierung des Datenschutzrechts

3.1.1 Europäisches Recht

Entwurf einer Datenschutz-Grundverordnung und einer Richtlinie 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 sowie zum freien Datenverkehr

Am 25. Januar 2012 hat die Europäische Kommission einen Entwurf einer Datenschutz-Grundverordnung (BR-Drs. 52/12) und eines Vorschlages für eine Richtlinie 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 sowie zum freien Datenverkehr (BR-Drs. 51/12) vorgelegt. Mit diesen Entwürfen sollen die Regelungen der bisher geltenden Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie des Rahmenbeschlusses 2008/977/JI, der den grenzüberschreitenden Datenverkehr für die Polizei und Strafverfolgungsbehörden regelt, überarbeitet werden und somit das Datenschutzrecht auf europäischer Ebene modernisiert und vereinheitlicht werden (vgl. zu wesentlichen Inhalten den Überblick der zuständigen Kommissarin der Europäischen Kommission Reding in ZD 2012, 195; weitere Details bei Hornung, ZD 2012, 99).

Durch dieses große Projekt der Europäischen Kommission soll es gelingen, die geltenden Datenschutzvorschriften, welche zum Teil fast zwanzig Jahre bestehen, an die fortschreitende technische Entwicklung anzupassen und die Vorschriften so zu gestalten, dass sie auch bei weiterem Fortschreiten der technischen Entwicklung einen europaweiten Standard bilden. Des Weiteren wird durch dieses Projekt erreicht, dass bei voranschreitender auch europaweiter Datenverarbeitung der Rechtsrahmen, un-

ter welchem die Datenverarbeitung, Datennutzung und Datenübermittlung erfolgen kann, einheitlich geregelt ist (vgl. X. Tätigkeitsbericht, Nr. 3.1).

Grundsätzlich wird somit die Modernisierung des europäischen Datenschutzrechts von den Datenschutzbeauftragten des Bundes und der Länder unterstützt, was auch in der Entschließung „Ein hohes Datenschutzniveau für ganz Europa!“ (**Anlage 11**) in der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam bekräftigt wurde.

Am 11. Juni 2012 trafen sich die Datenschutzbeauftragten des Bundes und der Länder zu einer Sonderkonferenz, um gemeinsame Stellungnahmen zur Datenschutz-Grundverordnung und zur Richtlinie 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 sowie zum freien Datenverkehr zu erarbeiten, welche auch an Frau Reding, die zuständige EU-Kommissarin, weitergeleitet wurden (siehe Homepage des Landesbeauftragten, Rubrik Internationales).

In der Stellungnahme zur Datenschutz-Grundverordnung wiesen die Datenschutzbeauftragten auf Kernpunkte hin, welche Ihrer Meinung nach unbedingt bei den weiteren Gesprächen zu beachten seien. So sei vor allem bei einer Harmonisierung des Datenschutzrechts ein möglichst hohes Datenschutzniveau für alle Mitgliedstaaten vorzuschreiben. Des Weiteren seien delegierte Rechtsakte auf das erforderliche Maß zu reduzieren. Technische und organisatorische Maßnahmen, welche zu treffen sind, um den Datenschutz zu gewährleisten, müssten sich auch in Zukunft am jeweiligen Stand der Technik orientieren. Die Möglichkeit der Verarbeitung von personenbezogenen Daten zur Profilbildung müsste in konkreten Regelungen festgeschrieben sein, vor allem bei Minderjährigen sei sie zu verbieten. Da es in den EU-Mitgliedstaaten kein einheitliches Verwaltungsverfahrens-, Verwaltungsprozess- und Verwaltungsvollstreckungsrecht gibt, sei die Regelung der „One-Stop-Shops“ für die Datenschutzaufsichtsbehörden nur praktikabel, wenn sie nicht als ausschließliche Zuständigkeit zu verstehen sei. Das beabsichtigte Kohärenzverfahren würde die Aufsichtsbehörden in deren Unabhängigkeit beeinträchtigen und verstoße damit sogar gegen die europäische Rechtsprechung.

Auch die Stellungnahme zum Entwurf einer Richtlinie wurde mit konkreten Forderungen versehen – z. B. Garantie eines hohen Datenschutzniveaus durch Mindeststandards. Des Weiteren sollte der Grundsatz der Erforderlichkeit klar definiert und eine Verpflichtung festgeschrieben werden, dass bei der Datenverarbeitung auch technische und organisatorische Maßnahmen zu treffen sind. Die Möglichkeiten der Mitgliedstaaten, die Rechte Betroffener einzuschränken, müssten reduziert werden. Als nicht hinnehmbar wurde die Möglichkeit angesehen, bei bestimmten Datenkategorien die Information bzw. die Auskunft an den Betroffenen ohne Abwägung im Einzelfall auszuschließen. Die Vorschriften über die Datensicherheit sollten um Datenschutzzielbestimmungen ergänzt werden und die Ausnahmeregelungen zu den Datenübermittlungsvorschriften in Drittländer

oder an internationale Organisationen müssen enger gefasst werden. So sollten auch im Richtlinienentwurf enthaltene Ausnahmen gestrichen werden, da anderenfalls fast jede Übermittlung darauf gestützt werden könnte, und dann eine Information an die Person, deren Daten übermittelt wurden, entfallen würde.

Der Landesbeauftragte beteiligte sich an den Erörterungen, u. a. bei einer Anhörung durch Abgeordnete des Europäischen Parlaments in Brüssel. In die Diskussion zu diesem Reformvorhaben sind neben den Vertretern der Datenschutzbehörden einschließlich der Art. 29-Gruppe auch Vertreter der Wissenschaft, der Wirtschaft und der Interessenverbände eingebunden. Auch Bundesrat und Bundestag (BT-Drs. 17/11325, angenommen 13. Dezember 2012) haben – zum Teil kritisch – Stellung genommen. Es zeigte sich, dass die Schaffung einer europäischen Rechtsgrundlage für den Datenschutz von sehr hohem Interesse ist. Jedoch sind in dieser Hinsicht auch unterschiedliche Tendenzen zu erkennen. Da die Regelungen der Datenschutz-Grundverordnung automatisch in jedem Land der Europäischen Union gelten, gibt es Bestrebungen, diese Anforderungen so niedrig wie möglich zu halten. Dies widerspräche jedoch den Interessen der Länder, die, wie z. B. Deutschland, bereits jetzt ein hohes Datenschutzniveau durch ihre Gesetze garantieren. Das Bundesinnenministerium verfolgte aber lange Zeit noch eine retardierende Linie mittels einer Betonung von Selbstregulierungsansätzen durch die Wirtschaft und eines Reduzierens des Datenschutzes bei weniger gefahrgeneigten Alltagsgeschäften.

Grundsätzlich befürworten die Datenschutzbeauftragten des Bundes und der Länder in der Entschließung der 84. Konferenz am 7./8. November 2012 in Frankfurt/Oder, dass ein einheitliches Datenschutzrecht für den öffentlichen Bereich und den nicht-öffentlichen Bereich gilt (**Anlage 16**). Für den öffentlichen Bereich wird von den Datenschutzbeauftragten des Bundes und der Länder des Weiteren nochmals bekräftigt, dass in der Datenschutz-Grundverordnung Mindestanforderungen festgelegt werden sollen und den jeweiligen Mitgliedstaaten die Möglichkeit eingeräumt wird, ein höheres Schutzniveau durch einzelstaatliche Regelungen zuzulassen. Das stärkt den Subsidiaritätsgedanken und bekräftigt die Verfassungsidentität der Mitgliedstaaten.

Diesen letzteren Gedanken hat das Bundesverfassungsgericht in seiner Entscheidung zur Antiterrordatei (Urteil vom 24. April 2013, ZD 2013, 328) gleichfalls betont und sich dabei etwas trotzig von der Rechtsprechung des Europäischen Gerichtshofs (zuletzt im Fall Åkerberg Fransson, Urteil vom 26. Februar 2013, NJW 2013, 1415) distanziert.

Immer die aktuelle Diskussion zu den Vorschlägen der Europäischen Union zum vorgelegten Entwurf einer Datenschutz-Grundverordnung im Blick und auch die vorgestellten Änderungsvorschläge nicht außer Acht lassend verabschiedeten die Datenschutzbeauftragten des Bundes und der Länder auch in der 85. Konferenz am 13./14. März 2013 in Bremerhaven eine Entschließung „Europa muss den Datenschutz stärken“ (**Anlage 21**) mit entsprechenden Erläuterungen (**Anlage 22**) zu 10 Kernpunkten. In dieser Entschließung weisen die Datenschutzbeauftragten nochmals ausdrück-

lich auf ihre Befürchtungen hin, dass mit der neuen Datenschutz-Grundverordnung eine Absenkung des Datenschutzniveaus erfolgt. Dies ist aus einigen Änderungsvorschlägen ersichtlich, in denen vorgeschlagen wird, Grundanforderungen an die Datenverarbeitung zu streichen, um für wirtschaftliche Interessen größere Spielräume zu lassen. Die angestrebten Regelungen widersprächen jedoch auch den Forderungen des Europäischen Parlaments, welches eine Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert hatte. Auch diese Entschließung und die entsprechenden Erläuterungen wurden an die EU-Kommissarin Frau Reding übersandt.

Der zum Abschluss des Reformprozesses notwendige Trilog zwischen Europäischer Kommission, Europäischem Parlament und Ministerrat verzögerte sich infolge umfangreicher Änderungsvorschläge und langwieriger Beratungen im Ministerrat. Ein Gelingen des Vorhabens noch vor Ende der Wahlperiode des Parlaments im Mai 2014 ist zweifelhaft; der Trilog hatte im Oktober 2013 noch nicht begonnen. Eine Umsetzung des Vorhabens erfolgt wohl erst im Rahmen der Digitalen Agenda der EU ab 2015. Aufgrund der Überwachungsaffäre der Geheimdienste (vgl. Nr. 1) wird zusätzlich eine Meldepflicht für Unternehmen bei der Datenweitergabe diskutiert. Ein solcher Vorschlag ist im Paket des Innenausschusses des Parlaments für die Verhandlungen enthalten.

Europaratskonvention Nr. 108

Zeitgleich zur Diskussion um den Entwurf der Datenschutz-Grundverordnung und des Entwurfes einer Richtlinie 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 sowie zum freien Datenverkehr wurde mit der Überarbeitung des Übereinkommens Nr. 108 des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten begonnen. Die Europaratskonvention Nr. 108 ist ein Übereinkommen, welches den Schutz und den grenzüberschreitenden Austausch personenbezogener Daten regelt. Die Konvention wurde am 28. Januar 1981 verabschiedet und trat am 1. Oktober 1985 in Kraft. In der Konvention wurden Datenschutzgrundsätze festgelegt, die in das jeweilige Recht des Unterzeichnerstaates umgesetzt werden mussten, in denen die Verarbeitung personenbezogener Daten mit IT-Unterstützung geregelt wurden. Inzwischen wurde die Europaratskonvention Nr. 108 durch ein Zusatzprotokoll ergänzt.

Um die Europaratskonvention an den heutigen Stand der Technik anzupassen, wird eine Überarbeitung angestrebt. Ein Entwurf wurde im Juni 2012 zur Diskussion gestellt. Das bisherige Übereinkommen soll dadurch an die Entwicklungen der Informationsgesellschaft angepasst und die Durchsetzung von Standards verbessert werden. So werden in der Neufassung auch genetische und biometrische Daten einbezogen. Des Weiteren sollen bei Datenlecks und Datenverlusten nicht nur die Aufsichtsbehörden informiert werden, sondern auch die Betroffenen.

So ist es nicht verwunderlich, dass die Europäischen Datenschutzbehörden in ihrer Konferenz vom 16. bis 17. Mai 2013 in Lissabon eine Entschließung über die Zukunft des Datenschutzes in Europa (**Anlage 35**) fasste, in welcher die besonderen Möglichkeiten einer solchen Modernisierung herausgehoben wurden. Gleichzeitig bekräftigt die Konferenz die Notwendigkeit eines einheitlichen und robusten Datenschutzrechtsrahmens. Sie weist den EU-Gesetzgeber darauf hin, zur Vermeidung einer gefährlichen rechtlichen Lücke im Datenschutz unbedingt die Datenschutz-Grundverordnung und die Richtlinie gleichzeitig zu verabschieden. Aber auch die Entwicklung angemessener Schutzmechanismen und dabei auch die Stärkung der Rechte und der Unabhängigkeit der Datenschutzbehörden werden durch die Europäischen Datenschutzbeauftragten gefordert.

Transatlantische Freihandelszone

Auch an der Diskussion zur Einführung einer transatlantischen Freihandelszone sind die Datenschutzbeauftragten des Bundes und der Länder beteiligt. Dabei vertreten die Datenschutzbeauftragten die Auffassung, dass bei den Verhandlungen zwischen der Europäischen Union und den Vereinigten Staaten zur transatlantischen Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rechtsrahmen Beachtung finden müssen. Demzufolge fordern die Datenschutzbeauftragten des Bundes und der Länder sicherzustellen, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus entwickelten Standards bei den Verhandlungen berücksichtigt werden. Diese Forderung wurde auch nochmals durch eine Entschließung anlässlich der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. bis 14. März 2013 in Bremerhaven (**Anlage 26**) bekräftigt. Die Datenschutzbeauftragten sehen in der vorgeschlagenen Freihandelszone auch die Chance, international eine Erhöhung des Datenschutzstandards zu erreichen.

Bei der Konferenz der Europäischen Datenschutzbehörden vom 16. bis 17. Mai 2013 in Lissabon wurde eine Entschließung (**Anlage 36**) gefasst, in welcher die Datenschutzbeauftragten ebenfalls den wirtschaftlichen Nutzen einer transatlantischen Freihandelszone für beide Volkswirtschaften betonten. Dabei begrüßten die Teilnehmer die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz und bekräftigten, wie bereits die Datenschutzbeauftragten des Bundes und der Länder, die Auffassung, dass das in der Europäischen Grundrechtscharta verankerte Recht auf Datenschutz und die daraus abgeleiteten hohen Standards gefördert und eingehalten werden sollten.

In seiner Sitzung vom 7. Juni 2013 fasste der Bundesrat jeweils eine „Entschließung zum Freihandelsabkommen zwischen der Europäischen Union und ihren Mitgliedstaaten einerseits sowie den USA andererseits (Transatlantic Trade and Investment Partnership – TTIP)“ (BR-Drs. 463/13) und eine „Entschließung zur Aufnahme von Verhandlungen zwischen der EU und den USA über ein transatlantisches Handels- und Investitionsabkommen (TTIP)“ (BR-Drs. 464/13). Beiden Entschließungen ist

zu entnehmen, dass ein transatlantisches Freihandelsabkommen begrüßt wird, jedoch die Bundesregierung aufgefordert wird, dafür Sorge zu tragen, dass geltendes Recht in Europa und vor allem in Deutschland nicht unterlaufen werde. Hier wurde als Beispiel das bereits bestehende hohe Rechtsschutzniveau in Europa aufgeführt.

Für den Herbst 2013 sind in Brüssel und Washington weitere Verhandlungsrunden zum Abkommen geplant.

Safe Harbor

Vom amerikanischen Handelsministerium wurden im Juli 2000 die Grundsätze des „sicheren Hafens“ zum Datenschutz vorgelegt. Diese wurden in einer Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglich „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG) (ABl. L 215 vom 25. August 2000, S. 7), bewertet.

In diesem Papier wurden Grundsätze festgelegt, wie eine Organisation Daten, welche sie erhält, zu schützen hat. Des Weiteren sind die rechtlichen Konsequenzen bei Nichtbeachtung aufgeführt. Dem Ganzen liegt zugrunde, dass nach der derzeit geltenden Datenschutzrichtlinie von 1995 Datenübermittlungen in Drittländer nur unter der Voraussetzung erlaubt sind, dass in dem Drittstaat ein angemessenes Schutzniveau gewährleistet wird. Die Europäische Kommission kann prüfen, ob ein Drittstaat diese Anforderung erfüllt. Somit hat die USA durch die Festlegung der Grundsätze des „Sicheren Hafens“ und der Führung eines Verzeichnisses der Unternehmen, welche sich auf die Grundsätze des Safe Harbors verpflichtet haben, Erleichterungen in der Datenübermittlung erreicht.

Da die US-amerikanischen Unternehmen die Zertifizierung durch eine Verpflichtung, sich an die Grundsätze des „Safe Harbor“ zu halten, selbst vornehmen, und eine Kontrolle weder durch die Kontrollbehörden in Europa noch in der USA erfolgt, wurden bereits 2010 Unternehmen in Deutschland durch den Düsseldorfer Kreis aufgerufen, „gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein in der Safe-Harbor-Liste geführtes US-Unternehmen übermitteln“.

Die in der jüngsten Vergangenheit bekannt gewordenen Informationen zu umfassenden und anlasslosen Überwachungsmaßnahmen von ausländischen Geheimdiensten zeigen, dass gerade in diesen Fällen ein angemessenes Datenschutzniveau nicht gewährleistet wurde und wird. In einer gemeinsamen Presseerklärung vom 24. Juli 2013 fordern daher die Datenschutzbeauftragten des Bundes und der Länder von der Bundesregierung eine Begrenzung des Zugriffs ausländischer Geheimdienste. Des Weiteren sollen Datenübermittlungen an Drittstaaten ausgesetzt werden, bis ein angemessener Datenschutz sichergestellt werden kann. Die Datenschutzbeauftragten des Bundes und der Länder gehen davon aus, dass auch gerade bei den Verhandlungen zur transatlantischen Freihan-

delszone solche Regelungen mit aufgenommen werden, dass Zugriffe von öffentlichen Stellen in den USA auf personenbezogene Daten nur unter den Voraussetzungen der Verhältnismäßigkeit, der Erforderlichkeit und der Zweckbindung erfolgen dürfen.

Der Landesbeauftragte wird die Entwicklungen in diesen Bereichen auch weiterhin aktiv begleiten.

3.1.2 Beschäftigtendatenschutz

Bereits im X. Tätigkeitsbericht (Nr. 3.1.2) hat der Landesbeauftragte die Entwicklung der Verbesserung des Beschäftigtendatenschutzes beschrieben. Der Gesetzentwurf der Bundesregierung vom Dezember 2010 (BT-Drs. 17/4230) sah vor, mit der Neuregelung der §§ 32 ff. BDSG für zahlreiche Fragen zum Beschäftigtendatenschutz klare Regelungen vorzugeben. Unter Beachtung des Informationsinteresses des Arbeitgebers sollten die Beschäftigten vor der unrechtmäßigen Erhebung personenbezogener Daten geschützt werden. Regelungen wurden vorgesehen zur Datenerhebung ohne Kenntnis der Beschäftigten zur Aufdeckung und Verhinderung von Straftaten, zur Videobeobachtung, zu Ortungssystemen, zur Erhebung von Daten mittels biometrischer Verfahren, zur Nutzung von Telekommunikationsdiensten (wie z. B. der Recherche von Bewerberdaten im Internet) oder zur Beschränkung der Nutzung der Einwilligung des Beschäftigten als Rechtsgrundlage der Datenerhebung.

Der Gesetzentwurf brachte aus datenschutzrechtlicher Sicht ein höheres Maß an Rechtssicherheit und inhaltlichem Niveau. Die vorgesehenen Regelungen nahmen einzelne datenschutzrechtliche Forderungen auf und stärkten in einigen Bereichen das informationelle Selbstbestimmungsrecht. Andererseits bestand vielfach erheblicher Verbesserungsbedarf. Als ein Beispiel sei die Videoüberwachung von Betriebsstätten genannt. Die nach bisheriger Rechtsprechung in notwehrähnlichen Situationen sinnvollerweise zugelassene heimliche Videoüberwachung wäre verboten, dafür wurde der Katalog der zulässigen erkennbaren Beobachtung sehr weit gefasst. Die Datenschutzbeauftragten des Bundes und der Länder haben daher am 25. Januar 2013 die Entschließung „Beschäftigtendatenschutz nicht abbauen, sondern stärken!“ gefasst (**Anlage 20**).

Der Gesetzentwurf wurde in den Ausschüssen des Bundestages behandelt. Eine Sachverständigenanhörung fand statt. Auch in der Öffentlichkeit wurden die beabsichtigten Regelungen sehr kontrovers diskutiert. Zu Beginn des Jahres 2013 sollte der Gesetzentwurf nach Änderungsvorschlägen der Regierung wieder auf die Tagesordnung kommen. Leider ist dies nicht geschehen, sodass der Entwurf der Diskontinuität unterlag.
Die EU-Datenschutz-Grundverordnung hat den Beschäftigtendatenschutz nicht im Fokus. Artikel 82 des Entwurfs gestattet den Mitgliedstaaten, in gewissem Rahmen gesetzliche Ausgestaltungen vornehmen zu können. Die EU-Kommission kann jedoch Durchführungsvorschriften erlassen.

3.1.3 Stiftung Datenschutz

Im X. Tätigkeitsbericht (Nr. 3.1.4) hatte der Landesbeauftragte die Entwicklung des Vorhabens der Bundesregierung beschrieben, eine Stiftung Datenschutz mit den Zielen einzurichten, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, ein Datenschutzaudit zu entwickeln, Bildung im Bereich des Datenschutzes zu fördern und den Selbstdatenschutz durch Aufklärung zu stärken. Der Bundestag hat bereits im Juni 2012 die Voraussetzungen für die Errichtung beschlossen. Einer Einladung des Bundesministeriums des Innern, drei Mitglieder in den Beirat der Stiftung zu entsenden, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder jedoch nicht entsprochen. Die Notwendigkeit enger Kooperation der Stiftung mit den Datenschutzbeauftragten und die völlige Unabhängigkeit, finanziell wie personell, bei der Wahrnehmung der Aufgaben war bereits in der Entschließung vom November 2010 gefordert worden (siehe X. Tätigkeitsbericht, Nr. 3.1.4). Gerade diese letztere Voraussetzung war nach Einschätzung der Datenschutzbeauftragten im November 2012 infolge der seinerzeitigen Konstruktion der Stiftung nicht erfüllt (vgl. Wagner, DuD 2012, 825), sodass von dem satzungsmäßigen Recht zunächst nicht Gebrauch gemacht wird. Die Stiftung nahm Anfang 2013 ihre Arbeit in Leipzig auf.

3.1.4 Änderung DSG LSA 2011

Der Werdegang der Umsetzung der **völligen Unabhängigkeit der Datenschutzaufsicht** durch den Landesbeauftragten nach den Vorgaben der Rechtsprechung des Europäischen Gerichtshofs wurde im X. Tätigkeitsbericht (Nr. 3.2) ausführlich dargestellt. Die Entwicklung hat zunächst mit den Regelungen des Zweiten Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 27. September 2011 (GVBl. LSA S. 648) ihr Ende gefunden (Änderung der Verwaltungsvorschriften in MBl. LSA 2012 S. 583).

Die Neuregelung sieht vor, dass der Landesbeauftragte der Dienstaufsicht des Präsidenten des Landtages nur unterliegt, soweit seine Unabhängigkeit nicht beeinträchtigt wird. Weiter wurde auf Vorschlag des Landesbeauftragten vorgesehen, dass die Bediensteten nur im Einvernehmen mit ihm versetzt oder abgeordnet werden können und ausschließlich an seine Weisungen gebunden sind; eine mittelbare Beeinflussung sollte so ausgeschlossen werden (§ 21 Abs. 1 Satz 4, Abs. 3 Sätze 4 und 5 DSG LSA).

Das Urteil des Europäischen Gerichtshofs vom 16. Oktober 2012 zur Österreichischen Datenschutzkommission (Az.: C-614/10, ZD 2012, 563) hat auf denkbare Einflüsse in Bezug auf die Personalausstattung durch Dienstaufsicht hingewiesen. Durch die vorgenannten Neuregelungen könnte jedoch auch diesen Anforderungen Rechnung getragen sein.

In § 22 DSG LSA wird nunmehr festgelegt, dass der Landesbeauftragte **Aufsichtsbehörde nach § 38 BDSG** ist. Er führt daher auch das Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1 BDSG. Nach § 4d Abs. 1 Satz 1 BDSG

müssen Unternehmen grundsätzlich Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde melden. Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat (§ 4d Abs. 2 BDSG). Für die Unternehmen im Land ist die Meldepflicht bedeutsam, da eine unterlassene oder fehlerhafte Meldung einen Ordnungswidrigkeitentatbestand nach § 43 Abs. 1 Nr. 1 BDSG erfüllen kann.

In dem neuen § 22 Abs. 2a DSG LSA wird dem Landesbeauftragten zudem die Verfolgung und Ahndung von dort benannten Ordnungswidrigkeiten, insbesondere nach § 43 BDSG, übertragen.

Dem Vorschlag des Landesbeauftragten, eine Datenschutzkommission einzurichten, wurde nicht gefolgt.

3.1.5 Novellierung DSG LSA 2013

Über die Unabhängigkeit der Datenschutzaufsicht hinaus erläuterte der Landesbeauftragte im X. Tätigkeitsbericht (Nr. 3.1.1) den Bedarf weiterer Novellierung des DSG LSA. Im Beschluss des Landtags von Sachsen-Anhalt vom 8. September 2011 (LT-Drs. 6/388) wurde ebenfalls das Anliegen der Modernisierung und Verbesserung des DSG LSA formuliert. Dies wurde mit Beschluss vom 19. Oktober 2012 (LT-Drs. 6/1545) bekräftigt.

Der Landesbeauftragte wurde vom Ministerium für Inneres und Sport bei der Erstellung des Referentenentwurfs zur Umsetzung dieser Vorgaben beratend beteiligt. Auch wenn wegen absehbarer Einflüsse durch europäisches Recht nicht alle wünschenswerten Aspekte aufgegriffen wurden, fanden seine Empfehlungen entsprechenden Eingang in den Entwurf. Unter anderem werden Regelungen zu gemeinsamen Verfahren (automatisierte Verfahren mehrerer verantwortlicher Stellen gemeinsam) getroffen, die Vorschriften zur Datenverarbeitung im Auftrag an die Anforderungen im BDSG angepasst, einschließlich einer Regelung zur Nutzung von „Cloud Computing“, und die Stellung des behördlichen Datenschutzbeauftragten gestärkt (Abberufung nur aus wichtigem Grund entsprechend § 626 BGB). Ein Fortschritt ergibt sich auch aus einer Regelung zur Informationspflicht bei Datenpannen, wie es sie schon in § 42a BDSG gibt. Ebenso bedeutend ist die an andere Datenschutzgesetze angelehnte Regelung, wonach die Anrufung des Landesbeauftragten bei Anhaltspunkten für Datenschutzverstöße auch dann zulässig ist, wenn keine eigene Betroffenheit besteht.

3.2 Europäische und internationale Entwicklungen

3.2.1 System der Bankdatenauswertung

In seinem X. Tätigkeitsbericht (Nr. 7.2) ist der Landesbeauftragte ausführlich auf die datenschutzrechtlichen Bedenken im Zusammenhang mit dem bestehenden Abkommen zu SWIFT und der damit verbundenen Datenübermittlung an die USA eingegangen.

Bei Kontrollen der Datenübermittlungen wurde durch die Gemeinsame Kontrollinstanz (GKI) Europol bereits im Jahr 2011 festgestellt, dass zu einigen Abfragen nicht geprüft werden könne, ob sie verhältnismäßig seien, da die Begründungen für die Anfragen fehlten oder unzureichend seien. Da die Berichte der GKI jedoch als geheim eingestuft wurden, dürfen sie auch nicht veröffentlicht werden und können somit auch nicht überprüft werden, nicht einmal durch das europäische Parlament.

Durch die EU-Kommissarin Cecilia Malmström wurden Eckpunkte für ein neues „Terrorist Finance Tracking System“ (TFTS) veröffentlicht, dass in Europa anstatt des bisherigen TFTP der USA eingerichtet werden soll.

Der Bundesrat hat mit Beschluss (BR-Drs. 415/11) vom 23. September 2011 ein neues EU-System befürwortet. Dabei betonte der Bundesrat, dass das Ziel eines solchen neu zu entwickelnden EU-Systems sein muss, ohne eine massenhafte Übermittlung von Zahlungsverkehrsdaten auszukommen.

Seitdem sind keine weiteren Bestrebungen zur Einführung eines neuen Systems zu beobachten.

Das Europäische Parlament setzte im Oktober 2013 ein politisches Signal: Da die NSA angeblich auch auf die SWIFT-Daten zugreife, solle das Abkommen ausgesetzt werden.

3.2.2 FATCA

Im Jahr 2010 ist in den USA ein Gesetz über die Steuerehrlichkeit bezüglich Auslandskonten („Foreign Account Tax Compliance Act“ – FATCA) in Kraft getreten. Mit diesem Gesetz wurden Meldepflichten der Finanzinstitute in Bezug auf die Konten, mit denen in den USA steuerpflichtige Personen und Gesellschaften ihre Steuern verkürzen könnten, eingeführt.

Zur Umsetzung dieser geforderten Meldepflichten schlossen die USA mit verschiedenen europäischen Partnerländern wie Deutschland, Frankreich Großbritannien, Italien und Spanien ab Juli 2012 bilaterale Abkommen.

Zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika wurde ein solches Abkommen am 31. Mai 2013 unterzeichnet, durch welches der gegenseitige Datenaustausch der Finanzinstitute mit den jeweiligen Steuerbehörden ab dem 1. Januar 2014 geregelt werden soll.

Die Umsetzung des Abkommens hat indes einige datenschutzrechtliche Fragen aufgeworfen. Unklar war vor allem, auf welcher Rechtsgrundlage eine Datenübermittlung stattfinden dürfe. Um diese für die Bundesrepublik Deutschland zu schaffen, soll eine Regelung in der Abgabenordnung aufgenommen werden, welche eine Vorbildfunktion für alle anderen internationalen Abkommen haben wird. Des Weiteren sollen in einer Durchführungsvereinbarung zum FATCA-Abkommen weitere datenschutzrechtliche Anforderungen festgeschrieben werden.

3.2.3 Flugpassagierdaten und Körperscanner

Ein Thema, mit welchem sich der Landesbeauftragte seit Jahren beschäftigen musste, ist die Speicherung und Übermittlung von Flugpassagierdaten bzw. PNR (vgl. X. Tätigkeitsbericht, Nr. 7.4).

Im November 2011 legte die Europäische Kommission einen erneuten Beschlussentwurf für ein Abkommen der Europäischen Union mit den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen vor. Durch dieses Abkommen soll für die Datenübermittlung an das United States Department of Homeland Security eine einheitliche Rechtsgrundlage innerhalb der Europäischen Union geschaffen werden. Trotz heftiger Kritik aus Datenschutzkreisen an der sehr langen Vorratsdatenspeicherung – fünf Jahre in einer aktiven Datenbank und weitere zehn Jahre in einer ruhenden Datenbank –, sowie an den Rechtsschutzmöglichkeiten nur nach US-amerikanischem Recht auch für europäische Bürger, ist das Abkommen im Sommer 2012 verabschiedet worden. Positiv an diesem Abkommen ist aus datenschutzrechtlicher Sicht die darin enthaltene Zweckbindung der Verwendung der PNR.

Dieses Abkommen sollte nach Willen der Europäischen Kommission auch als Vorbild für weitere Abkommen dieser Art gelten.

Das Europäische System zur Sammlung und Auswertung von Flugpassagierdaten, auf welches der Landesbeauftragte ebenfalls in seinem X. Tätigkeitsbericht (Nr. 7.4) hinwies, konnte aufgrund der massenhaften Kritik bisher gestoppt werden. Der Entwurf einer solchen Richtlinie begegnet vor allem auch verfassungsrechtlichen Bedenken. So wird durch eine automatisierte Auswertung und Analyse durch die Polizei und Strafverfolgungsbehörden sowie durch die geplanten Datenabgleiche die Möglichkeit einer anlasslosen Rasterfahndung eröffnet. Auch die angestrebte verdachtslose Speicherung aller Flugpassagierdaten auf Vorrat verstößt gegen die Rechtsprechung des Bundesverfassungsgerichts.

Seit Dezember 2012 ist auf dem Frankfurter Flughafen eine neue Generation Körperscanner im Einsatz. Nunmehr werden keine Nacktbilder der Personen mehr gezeigt, sondern es sind Piktogramme zu sehen, an welchen farblich die Bereiche markiert werden, an denen nochmals eine Sicherheitskontrolle durchgeführt werden soll. Die Benutzung der Körperscanner ist weiterhin freiwillig. Wer sie nicht verwenden möchte, wird weiterhin abgetastet. Da die bisher genutzten Körperscanner, über die noch im X. Tätigkeitsbericht (Nr. 7.4) berichtet wurde, viele Fehlalarme auslösten, so z. B. durch Schweißflecken oder einfache Falten in der Kleidung, wurde die Weiterentwicklung der Technik notwendig.

3.2.4 Schengener Informationssystem II

Das Schengener Informationssystem dient seit 1995 allen Sicherheitsbehörden der Staaten der Europäischen Union, die sich dem Schengener Abkommen angeschlossen haben, der automatisierten Personen- und Sachfahndung. In diesem System werden Personen gespeichert, die im

Schengen-Raum unerwünscht sind oder vermisst oder zur Fahndung ausgeschrieben werden (vgl. VII. Tätigkeitsbericht, Nr. 4). Darüber hinaus werden in diesem System aber auch Kraftfahrzeuge, die überwacht werden, gestohlene Ausweisdokumente und Schusswaffen, und Banknoten gespeichert. Da im Laufe der Zeit die Anzahl der gespeicherten Datensätze enorm in die Höhe gegangen ist, was auch an der Erweiterung des Schengen-Raumes liegt, und sich die Sicherheitsbehörden neue Funktionalitäten einforderten, beschloss die EU-Kommission 2001 die Entwicklung eines Schengener Informationssystems II (SIS II).

Nach mehrmaligen Verzögerungen erwartete die Europäische Kommission, die inzwischen für den Betrieb des Systems zuständig ist, die Inbetriebnahme des neuen Systems im Jahr 2010. Zu diesem Zeitpunkt gab es jedoch weiter bestehende Sicherheitslücken, welche die Nutzung des Systems ausschlossen. Aus diesem Grunde wurde das Gesamtprojekt in wesentlichen Teilen überarbeitet.

Im Juni 2011 einigte sich die Europäische Kommission darauf, dass eine IT-Agentur für Freiheit, Sicherheit und Recht mit Sitz in Tallinn – Hauptstadt von Estland – gebildet wird, welche vor allem für die Verwaltung des SIS II zuständig sein soll. Der Standort des Zentralrechners wird jedoch in Straßburg (Frankreich) bleiben, der des Backup-Systems in Österreich. Als neuer Termin für den Betrieb des SIS II wurde das erste Quartal 2013 genannt. Doch auch im Dezember 2012 waren die abschließenden vorgeschriebenen Tests noch nicht durchgeführt worden. So gab es beispielsweise Probleme, die Landesgrenze zwischen Finnland und Russland – immerhin über 1260 km – in die Schengen-Kontrollen einzubeziehen.

Im März 2013 wurde der Starttermin für SIS II bekanntgegeben. Das System konnte endlich am 9. April 2013 mit über sieben Jahren Verzögerung in Betrieb genommen werden. Für die datenschutzrechtliche Kontrolle ist nunmehr auch nicht mehr die Gemeinsame Kontrollinstanz Schengen neben den nationalen Aufsichtsbehörden zuständig, sondern der Europäische Datenschutzbeauftragte. Dazu wurde eine neue Kontrollgruppe gebildet, deren Sekretariat beim Europäischen Datenschutzbeauftragten angesiedelt ist.

„Smart Borders“

Mit Hilfe modernster Technologien will die EU laut Mitteilung der Europäischen Kommission Bürgerinnen und Bürgern aus Drittländern die Einreise in die EU erleichtern. Dieses System wurde „Smart Borders – Intelligente Grenzen“ genannt. In einem Einreise- und Ausreisesystem sollen die Einreise- und Ausreisedaten von Drittstaatenangehörigen für Kurzaufenthalte zentral gespeichert werden. Dabei sollen Daten über die Identität der Besucher, der Dauer und des Zwecks des Aufenthalts erhoben werden. Ziel ist es, in Zukunft auch biometrische Daten der Drittstaatenangehörigen zu erheben.

Mit diesem System würde eine neue, sehr umfangreiche Datenbank geschaffen werden. Die damit verbundenen Eingriffe in das Recht auf Privatsphäre, die sich daraus ergeben würden, müssten entsprechend der EU-Grundrechtecharta gerechtfertigt sein.

Die Artikel 29-Datenschutzgruppe kommt in ihrer Bewertung zu dem Ergebnis, dass der Grundrechtseingriff durch dieses System nicht gerechtfertigt wäre. Aber nicht nur bei den Datenschutzbeauftragten stößt dieses System auf Kritik. Auch einige EU-Abgeordnete kritisieren die verdachtsunabhängige Überwachung der Einreisenden, da sie sehr viel Geld kosten würde und zu befürchten sei, dass trotz Erfassung der ganzen Daten keine höhere Sicherheit zu erreichen sei.

3.2.5 Europäische Ermittlungsanordnung

Im Frühjahr 2010 haben sieben EU-Mitgliedstaaten einen Richtlinienvorschlag für eine europäische Ermittlungsanordnung vorgestellt. Der Vorschlag soll es den Mitgliedstaaten ermöglichen, Ermittlungen in anderen Mitgliedstaaten zu veranlassen oder Ermittlungsergebnisse anzufordern. Die angewiesene Behörde in einem anderen Mitgliedstaat hat die Ermittlungsmaßnahme automatisch und ohne weitere Prüfung umzusetzen. Die vorgeschlagenen Maßnahmen umfassen verdeckte Ermittlungen, Abfrage von Bankdaten, Telefonüberwachung, Observation, Festnahme, Durchsuchung und Anhörung von Zeugen. Im Frühjahr 2013 fanden Verhandlungen zwischen dem Europäischen Parlament und dem Rat der Europäischen Union statt.

Die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich vom 21. bis 22. März 2012 in Potsdam mit der europäischen Ermittlungsanordnung auseinandergesetzt. Hierbei kritisierte sie, dass die Ermittlungsanordnung dazu führen kann, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedsstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedsstaates zurückzuweisen, sind nicht immer ausreichend. Vor diesem Hintergrund hat die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (**Anlage 12**) gefordert, dass eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa nicht zulasten des Grundrechtsschutzes der Betroffenen gehen dürfe. Die Anforderungen der EU-Grundrechte-Charta seien konsequent einzuhalten. Die europäische Ermittlungsanordnung müsse in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Si-

cherheit und Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

3.2.6 Internationale Datenschutzkonferenzen

Die 33. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre fand vom 2. bis 3. November 2011 in Mexiko City statt. Sie stand unter dem Motto: „Datenschutz im globalen Zeitalter“. Im Rahmen dieser Konferenz wurde eine Entschließung zur datenschutzgerechten Verwendung des Internetprotokolls Version 6 (IPv6) gefasst (**Anlage 38**).

Die 34. Internationale Konferenz der Datenschutzbehörden vom 25. bis 26. Oktober 2012 in Punta del Este, Uruguay, stand unter dem Motto: „Persönlichkeitsschutz und Technologie im Gleichgewicht“. Hier wurden Entschließungen zum Thema Cloud Computing (**Anlage 40**), welche sechs grundlegende Empfehlungen für die Datenverarbeitung in der Cloud enthält, und über die Zukunft des Datenschutzes (**Anlage 39**) gefasst.

An der 35. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre vom 23. bis 26. September 2013 in Warschau nahm auch der Landesbeauftragte als deutscher Vertreter gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit teil. Dabei wurde unter anderem eine „Entschließung über digitale Bildung für alle“ (**Anlage 41**) gefasst. Weitere Schwerpunkte der Konferenz behandelten die Vermeidung von Profilen (**Anlage 42**) und das Thema Web Tracking (**Anlage 43**), und die Datenschutzbeauftragten forderten nicht zuletzt die „Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht“ (**Anlage 44**).

3.2.7 Europäische Datenschutzkonferenzen

Die Frühjahrskonferenz der europäischen Datenschutzbeauftragten vom 3. bis 4. Mai 2012 in Luxemburg widmete sich vorrangig der europäischen Datenschutzreform. Hierzu fasste sie einen Beschluss (**Anlage 34**), welcher nochmals die Hauptziele der Datenschutzreform bekräftigte, die bereits erreichten Verständigungen im Bereich der Datenverarbeitung lobte sowie auf noch erforderliche Verbesserungen in den Regelungen der Datenschutz-Grundverordnung und der vorgeschlagenen Richtlinie für den Bereich der Polizei und Justiz hinwies.

Auf der Frühjahrskonferenz der europäischen Datenschutzbeauftragten vom 16. bis 17. Mai 2013 in Lissabon wurde wiederum eine Entschließung zur Zukunft des Datenschutzes in Europa (**Anlage 35**) gefasst. Des Weiteren befassten sich die europäischen Datenschutzbeauftragten mit der „Gewährleistung des Datenschutzes in einer transatlantischen Freihandelszone“ (**Anlage 36**) und forderten verbindliche Vorgaben zu Maßnahmen zum Schutz personenbezogener Daten und deren Durchsetzung. Außerdem wurde die Sicherstellung eines angemessenen Datenschutzni-

veaus bei Europol (**Anlage 37**) gefordert. Keinesfalls sollte es hingenommen werden, dass aufgrund einer neu zu schaffenden Rechtsgrundlage für die erweiterten Möglichkeiten zur Verarbeitung von personenbezogenen Daten durch Europol das bestehende Datenschutzniveau absinkt.

3.2.8 Europäischer Datenschutztag

Der Europarat hat den 28. Januar als jährlich zu begehenden Datenschutztag ausgerufen, um das Bewusstsein für den Datenschutz in Europa zu stärken (IX. Tätigkeitsbericht, Nr. 3.3). Demgemäß begingen die Datenschutzbeauftragten des Bundes und der Länder auch im Januar 2012 und 2013 diesen Tag mit einer zentralen Veranstaltung. Mit Vorträgen und Diskussionen von Fachleuten aus Politik, Verwaltung und Wissenschaft konnte öffentlichkeitswirksam über die Themen der Vorratsdatenspeicherung und der Europäischen Datenschutz-Grundverordnung informiert werden.

4 Technik, Organisation, Telekommunikation und Medien

4.1 IT-Planungsrat

Der Landesbeauftragte berichtete in seinem X. Tätigkeitsbericht (Nr. 1.3.1) ausführlich über die Bildung und die wesentlichen Aufgaben des IT-Planungsrates (IT-PLR), der nunmehr seit seiner Konstituierung am 22. April 2010 die IT-Koordinierung von Bund und Ländern im Sinne einer föderalen Zusammenarbeit wahrnimmt. Im X. Tätigkeitsbericht hatte der Landesbeauftragte in einem weiteren Beitrag (Nr. 4.2) auf spezifische Datenschutzthemen des IT-PLR hingewiesen, insbesondere gemäß seines Projekt- und Anwendungsplanes mit den darin festgelegten Steuerungs- und Koordinierungsprojekten sowie den Anwendungen, die teilweise auch für das Land Sachsen-Anhalt von Bedeutung waren bzw. noch sind. Für zwei Anwendungen des IT-PLR, d. h. E-Government- bzw. IT-Lösungen, die dauerhaft zur Unterstützung automatisierter Prozesse in der öffentlichen Verwaltung von Bund und Länder zum Einsatz kommen, dem Leistungskatalog (LeiKa) und dem Behördenfinder, liegt die Federführung weiterhin in Sachsen-Anhalt.

Mit dem Beschluss der Landesregierung vom 3. Mai 2011 über den Aufbau der Landesregierung und die Abgrenzung der Geschäftsbereiche waren die Aufgaben der Landesleitstelle IT-Strategie der Staatskanzlei und die Aufgaben zum E-Government in der Landesverwaltung des ehemaligen Ministeriums des Innern vollständig an das Ministerium der Finanzen, hier der neugeschaffenen Abteilung 6 (Informations- und Kommunikationstechnologie – IKT), übergegangen (MBl. LSA S. 217). Demzufolge erfolgt seitdem die Vertretung des Landes Sachsen-Anhalt im IT-PLR durch den dafür zuständigen Staatssekretär des Ministeriums der Finanzen. Mit einem weiteren Beschluss zur Gemeinsamen Geschäftsordnung der Ministerien – Allgemeiner Teil – vom 20. März 2012 (MBl. LSA S. 145) wurde die Funktion eines Beauftragten der Landesregierung für Informationstechnik (**CIO**) im dafür zuständigen Ministerium der Finanzen eingerichtet. Zugleich wurde mit diesem Beschluss dem CIO ein neues Gremium zur

Seite gestellt, der **IKT-Rat**. In ihm wirken seit seiner konstituierenden Sitzung am 6. Juni 2012 die zuständigen Staatssekretärinnen und Staatssekretäre der Ressorts mit, die strategische Entscheidungen für die Landesverwaltung treffen sollen; Schwerpunkte betrafen bislang allerdings nur die Vorbereitungen der Sitzungen des IT-PLR. Zugleich wurde der bisherige ständige Staatssekretärsausschuss „Informationstechnologie“ aufgelöst. Die Staatssekretärskonferenz befasst sich aber weiterhin regelmäßig mit dem Thema Informations- und Kommunikationstechnologie in der Landesverwaltung und ist zudem Deeskalationsgremium für Entscheidungen, über die auf der Ebene des IKT-Rates keine Einigung erzielt werden kann. Der IKT-Rat hat sich eine entsprechende Verfahrensordnung gegeben. Neben den Vertretern der kommunalen Spitzenverbände ist der Landesbeauftragte beratendes Mitglied im IKT-Rat.

Zur weiteren Unterstützung des IKT-Rates, insbesondere zur fachlichen Vorbereitung der Sitzungen des IT-Planungsrates, wurde als separates Gremium der IKT-Kreis am 31. Mai 2012 gebildet, in dem der Landesbeauftragte ebenfalls beratendes Mitglied ist. Der IKT-Kreis löste damit den ehemaligen IT-Koordinierungsrat, der sich aus den IT-Referenten der Ressorts zusammensetzte, ab.

Der aktuelle Aktionsplan des IT-PLR 2013 vom 8. März 2013 (vormals Projekt- und Anwendungsplan) umfasst nachfolgendes Projekt- und Anwendungsportfolio und wird laufend fortgeschrieben:

Steuerungsprojekte des IT-PLR:

- **Informationssicherheit** (Leitlinie „Informationssicherheit“ für das ebenübergreifende E-Government) – Federführung: Bund,

- Open Government (Förderung des Open Government) – Federführung: Bund, Baden-Württemberg,

- **eID-Strategie** (Entwicklung und Umsetzung einer Gesamtstrategie für den Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government) – Federführung: Bund,

- FIM (Aufbau eines föderalen Informationsmanagements) – Federführung: Bund, Sachsen-Anhalt,

- DVDV 2.0 (neu) (Technologische Anpassung der Infrastruktur und zukunftssicherer Ausbau des Deutschen Verwaltungsdienstleverzeichnisses) – Federführung: Bund,

- Monitoring der Maßnahmen im E-Government (Dokumentation und öffentliche Darstellung von Maßnahmen der Umsetzung der NEGS) – Federführung: Geschäftsstelle IT-PLR.

Koordinierungsprojekte des IT-PLR:

- Nationales Waffenregister – Stufe 2 und 3 (neu) (Stufe 2: Einbeziehung von Händlern und Herstellern; Stufe 3: Geschäftsprozesse mit sicherer Authentifizierung durch den nPA) – Federführung: Bund, Baden-Württemberg; Auftraggeber: Innenministerkonferenz,

- S.A.F.E. (Weiterentwicklung des „Secure Access to Federated e-Justice/e-Government“) – Federführung: Baden-Württemberg, Rheinland-Pfalz; fachlich verantwortlich: Justizministerkonferenz,

- Moderne Bürgerdienste (Blaupause „Moderne Bürgerdienste – E-Government Infrastrukturen für eine bürgernahe Verwaltung im demografischen Wandel“) – Federführung: Sachsen, Mecklenburg-Vorpommern,

- Nationale Prozessbibliothek (Forschungsprojekt: Entwicklung einer Prozessbibliothek aller deutschen Verwaltungsprozesse mit einer Community-Plattform für die öffentliche Verwaltung) – Federführung: Bund,

- Prozessdatenbeschleuniger (P23R) (Ziel ist die Entwicklung von Methoden und offenen Standards für vernetzte und übergreifende Interprozessarchitektur für vereinfachten Datenaustausch zwischen Wirtschaft und Verwaltung) sowie deren Umsetzung in Pilotprojekten – Federführung: Bund,

- EDV-Grundbuch (neu) (Ziel: Neuentwicklung eines EDV-Grundbuches – Realisierung eines bundesweit einheitlichen Softwaresystems („Datenbank-Grundbuch“) und verbesserte Online-Beauskunftung) – Federführung: Bayern mit weiteren 5 Ländern; Basis bildet eine von allen 16 Ländern unterzeichnete Verwaltungsvereinbarung,

- Online Sicherheitsüberprüfung (OSip) (neu) (Ziel: einheitliche und länder- und fachbereichsübergreifende Durchführung von Zuverlässigkeits- und Sicherheitsüberprüfungen auf Basis einer Entwicklungs-Kooperation und eines gemeinsam finanzierten IT-Verfahrens) – Federführung: Nordrhein-Westfalen, Baden-Württemberg,

- Elektronische Rechnungsbearbeitung in der Verwaltung (E-Rechnung) (neu) (Ziel: Entlastungen und Vereinfachungen des elektronischen Rechnungsaustausches zwischen Unternehmen und öffentlicher Verwaltung sowie der anschließenden behördeninternen Rechnungsbearbeitung) – Federführung: Bund, Hessen,

- Cloud-E-Mail (neu) (Gemeinsame Infrastruktur für die Funktionen E-Mail, Kalender, Kontakte und Aufgaben) – Federführung: Hamburg,

- Nationale Langzeitspeicherung (Ziel: des Projektes ist es, einen gemeinsamen, übergreifenden Dienst für Langzeitspeicherung und Aussonderung von elektronischen Behördenunterlagen bereitzustellen) Federführung: Schleswig-Holstein, Beteiligung: Niedersachsen.

Maßnahmen zur Verbesserung der Rahmenbedingungen des E-Governments:

- Begleitung des E-Government-Gesetzes des Bundes – Federführung: Bund,

- Neufassung der Kieler Beschlüsse (Nachnutzung von IT-Verfahren) – Federführung: Hessen,

- Optimierung der Informations- und Kommunikationsbeziehungen des IT-Planungsrats (OptIK) – Federführung: Hessen, Sachsen,

- IT- und E-Government-Ausbildung von Fach- und Führungskräften der Verwaltung (E-Ausbildung) (neu) – Federführung: Hessen, Sachsen,

- Weitere Maßnahmen zur Verbesserung der Rahmenbedingungen (Bedarf an kurzfristig angelegten weiteren Maßnahmen, u. a. im Kontext der vom IT-Planungsrat beschlossenen Standardisierungsagenda (KoSIT) oder Prüfungen der Konsequenzen von Rechtsetzungsvorhaben z. B. aus dem Bereich der Europäischen Union).

Anwendungen des IT-PLR:

- Deutsches Verwaltungsdiensteverzeichnis (DVDV) (zentrale Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung zur Ermöglichung einer rechtsverbindlichen elektronische Kommunikation von und mit Behörden über die vorhandenen Fachverfahren) – Federführung: Bund,

- Behördenfinder Deutschland (BFD) (Der Behördenfinder Deutschland ist ein gemeinsamer Service der Portale über Verwaltungsgrenzen hinweg) – Federführung: Sachsen-Anhalt,

- Leistungskatalog (LeiKa) (Katalog von semantisch-standardisierten Bezeichnungen einschließlich deren Beschreibungen für ein einheitliches, vollständiges und umfassendes Verzeichnis der Verwaltungsleistungen über alle Verwaltungsebenen hinweg) – Federführung: Sachsen-Anhalt,

- Governikus (Mit der Lösung Governikus soll ein sicherer und nachvollziehbarer Datenaustausch durch öffentliche Verwaltungen (Bund, Länder und Kommunen) sowie Unternehmen und Einzelpersonen ermöglicht werden) – Federführung: Bremen,

- Behördennummer 115 (Schaffung eines einheitlichen telefonischen Zugangs zur Verwaltung für Bürgerinnen und Bürger durch Teilnehmer des 115-Verbundes und Einführung eines Ebenen übergreifenden Wissensmanagements) – Federführung: Bund.

Zwei datenschutzrelevante Steuerungsprojekte des IT-PLR für das E-Government, nämlich zur Informationssicherheit (Leitlinie Informationssicherheit) und zur eID-Strategie, die beide unter Federführung des Bundes stehen, werden in einem eigenen Beitrag (Nr. 4.3) einer kritischen Bewertung unterzogen.

4.2 E-Government und IKT-Strategie in Sachsen-Anhalt

Der Landesbeauftragte hatte in seinem X. Tätigkeitsbericht (Nr. 4.4) darauf hingewiesen, dass seitens der Landesregierung ein ihm avisierter E-Government-Maßnahmenplan 2010-2011 ausgeblieben war. Als Grund hierfür war zum einen die strukturelle Veränderung innerhalb der Landesregierung, d. h. der Verlagerung der Zuständigkeit und Verantwortlichkeit für die IT-Strategie und das E-Government im Land Sachsen-Anhalt zum Ministerium der Finanzen angeführt worden. Zum anderen wurde seitens der Landesregierung auf die am 24. September 2010 vom IT-Planungsrat in seiner 3. Sitzung verabschiedete Nationale E-Government-Strategie (NEGS) verwiesen, die nunmehr in einer zukünftigen E-Government-Strategie des Landes Berücksichtigung finden sollte.

Diese unbefriedigende Situation hat sicherlich auch das Parlament veranlasst, mit einem Beschluss – Sachsen-Anhalt digital – vom 12. Juli 2012 (LT-Drs. 6/1299) die Landesregierung aufzufordern, über den Stand der Planungen und die Umsetzung eines ganzheitlichen E-Governments in Sachsen-Anhalt für die gesamte Legislaturperiode, die mit den Aufgaben zur Modernisierung der Informationstechnik der Landesverwaltung und dem Struktur- und Aufgabenwandel der öffentlichen Verwaltung abgestimmt ist, zu berichten und bis zum 30. Dezember 2012 ein erstes Konzept hierzu vorzulegen. Dieses vorzulegende Konzept sollte u. a. nachfolgende Schwerpunkte enthalten:

- Entwurf einer E-Government-Strategie einschließlich des Standes der Umsetzung der E-Government-Maßnahmen der Jahre 2011 und 2012 sowie der geplanten Maßnahmen im Jahr 2013, die Koordinierung von Vorgaben der NEGS mit den Aktivitäten der Landesregierung sowie einen langfristigen Strategieansatz zur Organisation der Kooperation zwischen Kommunen und Land,

- Maßnahmenplan zur Lösung der infrastrukturellen Anforderungen im Land Sachsen-Anhalt (Breitbandausbau, Landesdatennetz),

- Einschätzung der datenschutzrechtlichen Anforderungen an E-Government-Verfahren.

In einer kurzfristig einberufenen Sondersitzung des IKT-Rates am 16. August 2012 wurde dann auch seitens des federführenden Ministeri-

ums der Finanzen der Entwurf einer IKT-Strategie für die Landesverwaltung vorgestellt. Der erfolgte Wechsel der Zuständigkeit für die IT-Strategie zum Ministerium der Finanzen wurde zum Anlass genommen, diese IT-Strategie neu auszurichten und mit der E-Government-Strategie zusammenzuführen. Im September 2012 informierte die Landesregierung das Parlament zur Umsetzung des Beschlusses des Landtages zur geforderten E-Government-Strategie (LT-Drs. 6/1459) mit dem Hinweis auf die Ausarbeitung und den Entwurf einer IKT-Strategie für die Landesverwaltung.

Am 16. Oktober 2012 wurde vom Kabinett die **IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“** als verbindliche Arbeitsgrundlage der Staatskanzlei und der Ressorts beschlossen (MBl. LSA S. 585). Gleichzeitig wurde damit das IT-Leitbild aus dem Jahr 2000 gegenstandslos. Der Beschluss der Landesregierung über die IT-Strategie vom 29. Juli 2008 (MBl. LSA S. 619) wurde aufgehoben. Nur die Anlagen 2 und 3 zum Beschluss von 2008 gelten allerdings als separate Richtlinien fort (betrifft Architekturempfehlung zum Namens- und Verzeichnisdienst sowie Empfehlung zu Standardsoftware).

An der Ausarbeitung der neuen IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“ wurde der Landesbeauftragte für den Datenschutz im Rahmen der Gremienarbeit des IKT-Kreises und des IKT-Rates beteiligt und hatte damit Gelegenheit, konstruktiv die Belange des Datenschutzes und der Datensicherheit mit einzubringen (siehe Nr. 1.5 Informationssicherheit und Datenschutz, Nr. 5.13 Informationssicherheitsmanagement und Datenschutz).

Die IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“ beschreibt nur allgemein die mittel- und langfristigen Handlungsschwerpunkte. Deshalb wird sie durch einen Umsetzungsplan ergänzt. In ihm erfolgt die Beschreibung der gegenwärtig 15 Projekte zur Umsetzung der IKT-Strategie. Die IKT-Strategie selbst soll fortgeschrieben und der Umsetzungsplan entsprechend jährlich kontrolliert werden.

Grundsätzlichen Handlungsbedarf zur zukünftigen Gestaltung einer modernen Landesverwaltung sah auch das Parlament. Seit März 2012 befasst sich eine Enquete-Kommission unter dem Thema „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“ gemäß Einsetzungsbeschluss vom 22. März 2012 (LT-Drs. 6/968) mit der Zukunft der öffentlichen Verwaltung und behandelt u. a. Themen wie Funktionalreform, Personalstruktur und E-Government sowie Open Government. Sie soll über einen Zeitraum von drei Jahren tätig sein und jährlich dem Parlament einen Zwischenbericht vorlegen.

Der Landesbeauftragte hat nach Aufforderung der Enquete-Kommission hierzu schriftlich, insbesondere zu Nr. III. 3. E-Government-Strategie des Einsetzungsbeschlusses Stellung genommen (Vorlage 8, ADrs. 6/E07/7 vom 15. April 2013) und seine Stellungnahme in der Anhörung der Enquete-Kommission des Landtages von Sachsen Anhalt am 19. April 2013 erläutert. Der Landesbeauftragte betonte dabei, dass Datenschutz stets

Grundrechtsschutz sei. Für einen effektiven Grundrechtsschutz sind technische und rechtliche Aspekte zusammen zu betrachten. Der Landesbeauftragte bemerkte in diesem Zusammenhang, dass der Eindruck bestehe, dass wichtige inhaltliche Fragen des E-Governments in Sachsen-Anhalt nur mit strukturellen Antworten versehen worden sind.

Als Fazit ist hier festzustellen:

- Mit den E-Government-Maßnahmenplänen der vergangenen Jahre wurden wesentliche Grundlagen (Basiskomponenten, Leitprojekte) für E-Government-Dienstleistungen geschaffen. Allerdings werden E-Government-Dienstleistungen von den Bürgerinnen und Bürgern nur genutzt werden, wenn sie entsprechendes Vertrauen in diese Dienste haben. An dieser Stelle sei an das fast schon fast „vergessene“ Urteil des Bundesverfassungsgerichtes vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) zur sog. „Online-Durchsuchung“ erinnert, welches damit den Anspruch auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ geschaffen hat, auch teilweise als „IT-Grundrecht“ bezeichnet. Dieses Grundrecht muss ausgefüllt werden. Der Staat muss den Bürgern glaubhafter vermitteln, dass ihm deren Rechte am Herzen liegen.

- Bei den E-Government-Maßnahmenplänen und so auch bei der IKT-Strategie Sachsen-Anhalt digital 2020 fällt auf, dass die Maßnahmen bzw. Projekte ganz überwiegend innerhalb der Verwaltung angesiedelt sind. Es fehlen Projekte im Verhältnis des Staates bzw. der Verwaltung gegenüber den Bürgerinnen und Bürgern. Insofern kann man durchaus davon sprechen, dass der Kerngedanke von E-Government in Sachsen-Anhalt kaum verwirklicht worden ist. Die neue IKT-Strategie Sachsen-Anhalt digital 2020 umfasst unterschiedliche Kategorien von Projekten; ein roter Faden einer E-Government-Strategie für die Bürgerinnen und Bürger sowie die Unternehmen ist darin nicht erkennbar (vgl. das erste Konzept der Landesregierung in LT-Drs. 6/1742 vom 11. Januar 2013).

- Insgesamt empfiehlt der Landesbeauftragte eine ganzheitliche, nachhaltige, verbindliche und vernetzte Strategie. Datenschutz und Datensicherheit müssen dabei eingehalten werden. Privacy by Design und Privacy by Default müssen bei Projekten mit umgesetzt werden.

- Eine Einbindung der kommunalen Ebene (gem. § 5 Verwaltungsmodernisierungsgrundsätzegesetz) ist für ein nachhaltiges E-Government unverzichtbar. Dieses sollte sich in einer neuen Rahmenvereinbarung des Landes mit den Kommunalen Spitzenverbänden widerspiegeln, die Ende 2013 abgeschlossen werden soll.

- Für die zukünftige Umsetzung einer E-Government-Strategie empfiehlt der Landesbeauftragte, auch ein E-Government-Gesetz des Landes zu schaffen.
  Durch das am 1. August 2013 in Kraft getretene Gesetz zur Förde-

rung der elektronischen Verwaltung (E-Government-Gesetz – EGovG) vom 25. Juli 2013 (BGBl. I S. 2749) besteht hier Handlungsbedarf. Der Geltungsbereich des Gesetzes erstreckt sich nur dann auf die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder und der Gemeinden und der sonstigen der Aufsicht der Länder unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen (§ 1 Abs. 2 EGovG).
Das EGovG sieht leider keine verbindlichen Regelungen zum Angebot einer Ende-zu-Ende-Verschlüsselung für die Kommunikation zwischen der Verwaltung und den Bürgerinnen und Bürgern vor. Dieses bereits im De-Mail-Gesetz angelegte Defizit besteht nun auch für den Bereich der elektronischen Verwaltung fort. Insbesondere bei der elektronischen Übermittlung von Sozialdaten und anderen sensitiven Daten (u. a. Gesundheitsdaten, Steuerdaten) ist das nicht akzeptabel (vgl. Roßnagel, NJW 2013, 2710).
Die Erstellung eines ressortübergreifenden „Masterplan E-Government-Gesetz“ durch das Bundesministerium des Innern, wie die Bundesregierung am 21. September 2012 in ihrer Antwort auf die Forderung des Nationalen Normenkontrollrates zum damaligen Entwurf des EGovG verlauten ließ, steht noch aus.

E-Government kann nur gelingen, wenn der Datenschutz dabei als Vertrauensfaktor begriffen wird und eine entsprechende Umsetzung erfährt.

4.3 Leitlinie für Informationssicherheit und eID-Strategie

Leitlinie für Informationssicherheit des IT-PLR

In ihrer Stellungnahme vom 28. März 2012 (LT-Drs. 6/997) zum X. Tätigkeitsbericht des Landesbeauftragten hatte die Landesregierung über die Absicht des IT-Planungsrates (IT-PLR), eine verbindliche Leitlinie für Informationssicherheit für den Bund und die Länder zu erarbeiten, informiert.

Damit wurde die Verabschiedung des unter Mitwirkung des Landesbeauftragten in der Arbeitsgruppe „Informationssicherheit“ unter Leitung der Staatskanzlei erarbeiteten Entwurfs einer Landesleitlinie Informationssicherheit (LL IS) im April 2011 ausgesetzt. In diesem Entwurf waren seine Empfehlungen, insbesondere zur Aufnahme datenschutzspezifischer Schutzziele wie Authentizität, Revisionssicherheit und Transparenz in die LL IS, berücksichtigt worden. Mit Fertigstellung der LL IS sollte die Beschlussfassung der Landesregierung zum Aufbau eines Informationssicherheitsmanagements im Land vorbereitet werden. Der Entwurf der LL IS (Stand Februar 2011) berücksichtigte die Belange des Datenschutzes und der Datensicherheit.

Das Land Sachsen-Anhalt beteiligte sich an der Ausarbeitung in der Kooperationsgruppe „Informationssicherheit“ des IT-PLR, konnte sich aber mit diesen guten Ansätzen zur Integration von Datenschutz und Datensicherheit, wie im damaligen Entwurf der LL IS, nicht durchsetzen. Auf der

10. Sitzung des IT-PLR am 8. März 2013 wurde die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ einschließlich des Umsetzungsplanes beschlossen. Sie ist ein wichtiger Bestandteil des Steuerungsprojektes Informationssicherheit des Aktionsplans 2013 des IT-PLR.

Ein grundsätzliches Problem dieser Leitlinie des IT-PLR besteht darin, dass das Konzept für die Informationssicherheit auf dem IT-Grundschutz des BSI basiert, datenschutzrechtliche Belange nicht ausreichend berücksichtigt werden und diese Leitlinie für den kommunalen Bereich nur empfehlenden Charakter trägt, obwohl sich die kommunalen Spitzenverbände für eine verbindliche Regelung ausgesprochen hatten.

Entsprechend der am 16. Oktober 2012 beschlossenen IKT-Strategie „Strategie Sachsen-Anhalt digital 2020“ (MBl. LSA S. 585) (Nr. 4.2) beabsichtigt das Ministerium der Finanzen nach der Sommerpause im Jahr 2013, die Ausarbeitung der Landesleitlinie Informationssicherheit unter Einbeziehung von Vertretern der kommunalen Spitzenverbände, des Landesbeauftragten und unter Beachtung der Leitlinie für Informationssicherheit des IT-PLR fortzusetzen. Ergebnisse sollen Ende des Jahres 2013 vorliegen. Die Verabschiedung dieser Landesleitlinie Informationssicherheit sollte in Hinblick auf den näher rückenden Termin der Inbetriebnahme eines Verbindungsnetzes durch den Bund, über das der Datenaustausch zwischen dem Bund und den Ländern ab dem 1. Januar 2015 erfolgen soll (§ 3 IT-NetzG), nicht verzögert werden. Die Umsetzung der Anforderungen aus der Leitlinie für Informationssicherheit des IT-PLR in Sachsen-Anhalt ist verbindliche Voraussetzung zum Anschluss an dieses Verbindungsnetz.

eID-Strategie des IT-PLR

Ein weiteres Steuerungsprojekt des IT-PLR, ebenfalls Bestandteil im Aktionsplan 2013 des IT-PLR, ist die Entwicklung einer Gesamtstrategie für den Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government – eID-Strategie für E-Government. Den Rahmen für die Ausarbeitung einer solchen Gesamtstrategie bildet das sog. Eckpunkte-Papier zu dieser eID-Strategie, beschlossen auf der 9. Sitzung des IT-PLR am 25. Oktober 2012.

Die öffentliche Verwaltung in Bund und Ländern stellt zwar zahlreiche Online-Dienste mit dem Ziel bereit, Vorgänge elektronisch abwickeln zu können. Nach wie vor beschränken sich allerdings die meisten dieser Dienste auf Informations- oder Download-Angebote. Rechtsverbindliche Transaktionsangebote, u. a. für Antragstellungen durch Bürgerinnen und Bürger und Bewilligungen durch die öffentliche Verwaltung, besitzen dagegen immer noch Seltenheitswert. Zum Teil existieren hierfür die erforderlichen Verfahren z. B. zur elektronischen Identifizierung und Signatur, werden aber aus unterschiedlichen Gründen entweder von Verwaltungen nicht angeboten oder von Unternehmen, Bürgerinnen und Bürgern nicht genutzt.

Zur Ausarbeitung einer gemeinsamen Strategie für die leichte Handhabung von elektronischen Identitäten (eID) und das flächendeckende Angebot von sicheren elektronischen Verfahren zur Gewährleistung von Identität, Authentizität, Integrität und Vertraulichkeit (sog. Vertrauensdienste) im E-Government wurde eine Projektgruppe „eID-Strategie“ mit der Ausarbeitung eines Strategie-Papiers für Bund, Länder und Kommunen beauftragt. Der Hessische Datenschutzbeauftragte wirkte beratend im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in dieser Projektgruppe mit. Nach seiner Einschätzung fand trotz intensiven Bemühens der Datenschutz weder in dem Eckpunkte-Papier noch in dem Strategie-Papier im erforderlichen Umfang Berücksichtigung.

Bereits die Nichtberücksichtigung des Datenschutzes als übergeordnetes Ziel neben den im Eckpunkte-Papier benannten Zielen Sicherheit, Akzeptanz und Wirtschaftlichkeit steht im Widerspruch zur im März 2013 verabschiedeten Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, in der neben den Schutzzielen der Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) auch auf die technisch-organisatorische Umsetzung des Datenschutzes hinsichtlich Transparenz, Betroffenenrechte und Zweckbindung Bezug genommen wird.

Welche grundsätzlichen Probleme bestehen, zeigt der Entwurf einer Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, in dem die Europäische Kommission neue Regelungen vorschlägt, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Der Landesbeauftragte hat hierzu im Rahmen der Anhörung nach Aufforderung der Enquete-Kommission schriftlich Stellung genommen (Vorlage 8, ADrs. 6/E07/7, vom 15. April 2013, Nr. 1.4.3 Probleme mit dem neuen Personalausweis (nPA)). Ein grundsätzliches Problem liegt z. B. darin, dass die eID-Funktion des nPA zwar datenschutzgerecht ausgestaltet ist, nach dem vorliegenden Verordnungsentwurf aber nicht notifiziert werden kann. Hier lautet nämlich die Forderung, dass die eID rund um die Uhr, ohne besondere Anforderungen an (zusätzliche) Hard- oder Software und kostenlos geprüft werden können muss. Das ist beim nPA nicht der Fall. Die datenschutzgerechten Funktionen des nPA sollten in diesen Entwurf der Verordnung mit eingebracht werden. Diese Verordnung soll, falls sie in Kraft treten würde, die europäische Signaturrichtlinie 1999/93/EG ersetzen. Zugleich hätte dann auch das deutsche Signaturgesetz keine Geltung mehr. Allerdings ist dieser Vorschlag der EU-Kommission für eine Verordnung vom Parlament noch nicht beschlossen worden.

Auch das eID-Strategie-Papier (12. Sitzung des IT-PLR, 2. Oktober 2013) berücksichtigt die grundsätzlichen Vorgaben der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung nicht in ausreichendem Maß. Die bloße Nennung eines Begriffs wie „Datenschutz“ im Strategie-Papier, neben den übergeordneten Zielen des Eckpunkte-Papiers Sicherheit, Akzeptanz und Wirtschaftlichkeit, ohne Untersetzung durch Maßnahmen in diesem Strategie-Papier ist damit nur Kosmetik.

Der Landesbeauftragte hatte empfohlen, die Verabschiedung dieser eID-Strategie des IT-PLR auszusetzen und die Beschlussfassung auf eine der nächsten Sitzungen zu vertagen, auch insbesondere unter dem Eindruck der im Jahr 2013 bekannt gewordenen umfangreichen Abhör- und Überwachungsskandale amerikanischer und britischer Geheimdienste (Nr. 1.3). Die Projektgruppe eID-Strategie soll bis Ende des Jahres 2016 weiter bestehen bleiben.

4.4 Zentraler IT-Dienstleister für Sachsen-Anhalt – Dataport

Es läuft der 4. Versuch einer Landesregierung, die Konsolidierung der Informationstechnik der Landesverwaltung und die Konzentration von Querschnittsdiensten mit dem Aufbau eines zentralen IT-Dienstleisters für die Landesverwaltung zu unterstützen. Im Jahr 1991 wurde im damaligen Landesamt für Landesvermessung und Datenverarbeitung (LVermD) ein Landesrechenzentrum eingerichtet, im Jahr 2002 ein Landesinformationszentrum Sachsen-Anhalt (LIZ), als LHO-Betrieb, durch Herauslösung des ehemaligen Landesrechenzentrums aus dem LVermD. Mit dem 1. September 2009 erfolgte die Gründung und ab 1. Januar 2010 die Zusammenführung des LIZ mit dem Finanzrechenzentrum der Oberfinanzdirektion (OFD) Magdeburg zum neuen Landesrechenzentrum (LRZ) als Abteilung 4 der OFD Magdeburg. Der Landesbeauftragte informierte zum Sachstand über den Aufbau des LRZ in seinem X. Tätigkeitsbericht (Nr. 4.3). Nach der Planung der Landesregierung soll durch den Beitritt des Landes Sachsen-Anhalt zum IT-Verbund der nordostdeutschen Länder, mit dem das Land Sachsen-Anhalt neben Schleswig-Holstein, Hamburg, Mecklenburg-Vorpommern, Bremen und Niedersachsen sechstes Trägerland und Miteigentümer der rechtsfähigen Anstalt des Öffentlichen Rechts „Dataport“ werden würde, die Etablierung eines zentralen IT-Dienstleisters erfolgen. Das LRZ soll danach gem. Artikel 2 des Entwurfs des Zustimmungsgesetzes zum Staatsvertrag zum 1. Januar 2014 in die rechtsfähige Anstalt des öffentlichen Rechts Dataport eingegliedert werden. Für Dataport ist eine Vollintegration aller Fachverfahren der Landesverwaltung geplant. Der Staatsvertrag soll nach Ratifizierung durch die Trägerländer rückwirkend zum 1. Januar 2013 in Kraft treten.

Mit dem Kabinettsbeschluss vom 8. Mai 2012 wurde der zuständige Staatssekretär des Ministeriums der Finanzen (CIO) beauftragt, die Gespräche über den Beitritt des Landes Sachsen-Anhalt zum IT-Verbund der norddeutschen Länder, der rechtsfähigen Anstalt des öffentlichen Rechts Dataport, fortzuführen, den Entwurf des Staatsvertrages mit den übrigen Trägerländern und den Ressorts abzustimmen und dem Kabinett zur Zustimmung vorzulegen. Der Verwaltungsrat von Dataport hatte in einem Beschluss vom 2. Mai 2012 der Ausarbeitung eines neuen Staatsvertrages zugestimmt.

Der Landesbeauftragte hatte in der Sitzung des IKT-Rates am 6. Juni 2012 zum Thema Dataport auf die dazu noch ausstehenden Informationen zu seiner rechtzeitigen Unterrichtung gem. § 14 Abs. 1 Satz 2 DSG LSA kritisch hingewiesen. Unter der Bezeichnung „Beitritt des Landes Sach-

sen-Anhalt zum IT-Trägerverbund der norddeutschen Länder“ (BeiST) ist dieses Projekt ein Umsetzungsvorhaben der neuen IKT-Strategie des Landes (Nr. 4.2). Eine erste Information über das Gesamtprojekt BeiST durch den CIO selbst erfolgte allerdings erst in einem Gespräch mit dem Landesbeauftragten am 13. September 2012.

Der Landesbeauftragte hatte im September 2012 einen Vorentwurf des Staatsvertrages kommentiert, das Ministerium der Finanzen sicherte eine weitere Beteiligung zu. Weitere Informationen zum aktuellen Sachstand (Analyse der zu übertragenden Fachverfahren, Prozesse, Teilpaketlösungen, Verwaltungsvereinbarung der Landesregierung mit Dataport, Details des IT-Betriebs), erreichten den Landesbeauftragten bis auf die Wirtschaftlichkeitsberechnung des Projektes BeiST nur spärlich.

Im Ergebnis eines weiteren Gespräches des CIO des Landes mit dem Landesbeauftragten am 24. Juli 2013 hatte dieser die Möglichkeit, zum Entwurf des Zustimmungsgesetzes zum Staatsvertrag Stellung zu nehmen.

Die Kontrollrechte des Landesbeauftragten gegenüber Dataport werden in § 15 des Entwurfs des Staatsvertrages geregelt und begegnen keinen grundsätzlichen Bedenken aus datenschutzrechtlicher Sicht. Dennoch ergeben sich für den Landesbeauftragten noch offene Fragestellungen zum Gesamtkomplex Dataport einschließlich des aktuellen Entwurfs zum Staatsvertrag (LT-Drs. 6/2468). Das betrifft z. B. die angestrebte Vollintegration zu Dataport, als zentraler IT-Dienstleister für das Land Sachsen-Anhalt (allerdings ohne das Landesdatennetz). Dem Landesbeauftragten liegt auf seine Anforderung hin seit August 2013 zumindest eine erste Übersicht der zur Migration zu Dataport anstehenden Fachverfahren vor. Diese Übersicht ist natürlich nicht abschließend und unterliegt einer ständigen Veränderung.

Beispielhaft sei hier auf das Projekt PROMIS (Personal-, Ressourcen-, Organisationsmanagement- und Informationssystem) hingewiesen, für das eine Fortsetzung der Gespräche mit dem Landesbeauftragten noch aussteht.
Das System PROMIS soll ressortübergreifend Aufgaben im Bereich der Personalverwaltung, der Personalentwicklung und -planung, der Dienstposten- und Arbeitsplatzverwaltung, der Stellenbewirtschaftung sowie der Verwaltung der Personalausgaben und der Personalkostenhochrechnung wahrnehmen. Der Landesbeauftragte begleitet seit dem Jahr 2005 den Prozess der Einführung dieses landesweiten Personalmanagementsystems und ist in der Projektlenkungsgruppe beratenes Mitglied. Wegen datenschutzrechtlicher und insbesondere beamtenrechtlicher Vorgaben müssen die Zugriffe auf die personenbezogenen Daten in der Verantwortung der jeweils datenschutzrechtlich verantwortlichen Stelle, der personalaktenführenden Stelle, verbleiben. Ein 1. Entwurf des Konzepts zu Berechtigungen und Datenschutz (Stand 26. Oktober 2010) in PROMIS wurde dem Landesbeauftragten vorgelegt.
Eine besondere Problematik hierbei ist die Notwendigkeit hinreichender Vorgaben des Datenschutzkonzepts zur dezentralen Verschlüsselung von

Daten oder Datensätzen. Der Landesbeauftragte hatte stets das Erfordernis einer Rechtsgrundlage für einen ressortübergreifenden Datentransfer betont. Im Rahmen der Neuregelung des Landesbeamtenrechts ist dem nicht mehr gesondert Rechnung getragen worden. Einem Datentransfer im Wege der Datenverarbeitung im Auftrag steht gem. § 3 Abs. 3 Satz 2 DSG LSA das Personalaktengeheimnis entgegen. Demgemäß ist eine Vorabverschlüsselung der zentral abgelegten Daten und deren verschlüsselte Übertragung und Speicherung in einer zentralen Datenbank geboten. Zu dieser Thematik trifft der 1. Entwurf des Konzepts allerdings keine konkreten Aussagen. Derzeit liegt dem Landesbeauftragten kein neues bewertungsfähiges Konzept vor.

Die hier am Beispiel von PROMIS aufgezeigten datenschutzrechtlichen Fragestellungen und Probleme könnten sich so oder ähnlich auch bei den zur Migration zu Dataport anstehenden Fachverfahren ergeben.

Grundsätzlich sind die Bestimmungen zur Auftragsdatenverarbeitung (§ 8 DSG LSA) bei diesem Migrationsprozess zu Dataport zu beachten. Zur Begründung eines Benutzerverhältnisses mit Dataport erfolgt hier in § 3 Abs. 1a des Entwurfs des Staatsvertrages der Verweis auf den öffentlich-rechtlichen Vertrag nach den §§ 121 bis 129 des Landesverwaltungsgesetzes Schleswig-Holstein. Es stellt sich die Frage, wie in diesem Zusammenhang dazu die angestrebte Beauftragung durch das Ministerium der Finanzen oder durch die Ressorts für bestimmte zu migrierende Fachverfahren im Sinne einer Auftragsdatenverarbeitung nach § 8 DSG LSA zu betrachten ist. Der Landesbeauftragte hatte hierzu auf Anfrage des Ministeriums der Finanzen vom 26. Juli 2013 Hinweise zu Entwürfen für eine Rahmenvereinbarung zum Datenschutz bei der Verarbeitung personenbezogener Daten von Behörden des Landes Sachsen-Anhalt durch Dataport und für eine Beauftragung von Dataport durch das Ministerium der Finanzen des Landes Sachsen-Anhalt bzw. das LRZ gegeben.

Unabhängig von einem geschlossenen Staatsvertrag und einer Beauftragung von Dataport als zukünftiger zentraler IT-Dienstleister für Sachsen-Anhalt 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 beim Auftragnehmer, hier bei Dataport. Es bestehen Zweifel an der pauschalen Regelung in § 3 Abs. 2 des *geltenden* Staatsvertrages, wonach sich Dataport zur Aufgabenerfüllung Dritter bedienen kann. Gemäß § 8 Abs. 2 Satz 2 DSG LSA wären solche Unterauftragsverhältnisse vorab schriftlich festzulegen und würden damit auch für die Subunternehmen von Dataport gelten. Die Hinweise in Nr. 2.3 (Unterauftragsverhältnisse) der Dataport Datenschutz-Leitlinie vom 25. März 2011 (Version 1.3) sind insofern als Maßgabe nicht ausreichend und besitzen zudem keine Gesetzeskraft.

Die Beteiligung des Landesbeauftragten in den IKT-Gremien des Landes ersetzt nicht dessen konkrete Unterrichtung bei der Planung und Änderung informationstechnischer Systeme gem. § 14 Abs. 1 Satz 2 DSG LSA. Die Planungsphase eines Projekts betrifft insbesondere auch das Ob der Einführung eines Systems; bereits dazu ist der Landesbeauftragte zu beteiligen. Eine solche frühzeitige Unterrichtung unterstützt einen vorgezogenen Grundrechtsschutz.

4.5 De-Mail

Bereits im X. Tätigkeitsbericht (Nr. 4.8) nahm der Landesbeauftragte das erst am 28. April 2011 erlassende De-Mail-Gesetz (BGBl. I S. 666) zum Anlass, mögliche Nachbesserungen für einen datenschutzgerechten Einsatz von De-Mail zu benennen. An den Hauptkritikpunkten hat sich leider nicht viel geändert. Eine Ende-zu-Ende-Verschlüsselung, also die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg, ist immer noch nicht Standard, jedoch vereinzelt mit unterschiedlichem Aufwand, teils gar manuellen Verschlüsselungen, möglich.

Die ersten Anbieter sind auf dem Markt und De-Mail-Adressen sind mittlerweile erhältlich. De-Mail macht den E-Mail-Versand sicherer, da zumindest eine Transportverschlüsselung sowohl zwischen den De-Mail-Providern untereinander als auch zu deren Nutzern erfolgt, nachvollziehbarer und auch nachweisbar. SPAM-De-Mails wird es wohl nicht geben, inwieweit Schadsoftware per De-Mail rechtzeitig erkannt werden kann, ist fraglich, da sie wohl sowieso nur speziell präpariert und getarnt verschickt werden würde. Jedenfalls wäre der Absender ermittelbar. Eine Ende-zu-Ende-Verschlüsselung für beispielsweise „nur Text“-Nachrichten wäre denkbar.

Bei aller Kritik bietet das De-Mail-System zumindest einige Vorteile. Es ist keine separate Hard- oder Software notwendig. De-Mails lassen sich per Webbrowser lesen und schreiben und werden relativ sicher transportverschlüsselt übertragen. De-Mail-Anbieter müssen sich einem Akkreditierungsverfahren stellen und werden dabei auch bezüglich der Einhaltung wichtiger Datenschutzmaßnahmen geprüft. Die Nutzer werden vorab identifiziert, können gleichzeitig aber auch unter Pseudonymen auftreten. Diese gesicherte Identität trifft auch auf Unternehmen und Behörden zu. Bei wichtigen Funktionen ist eine 2-Faktor-Authentisierung als Anmeldung notwendig. Es gibt Sende- und Empfangsbestätigungen.

Dass Dritte De-Mails u. U. mitlesen könnten, ist anzunehmen, dass Einzelpersonen gezielt Post abfangen und mitlesen, darf angezweifelt werden, da diese i. d. R. nicht über Filtertechnologie an den entsprechenden Stellen verfügen. Erst die Zukunft oder ein Whistleblower wird eventuell zeigen, wer Mittel und Wege finden wird, um sich Zugriff zu verschaffen. Derzeit sind Administratoren des jeweiligen De-Mail-Anbieters möglicherweise dazu in der Lage, obwohl seitens der De-Mail-Provider dies dementiert und auf detaillierte Zugriffsrechtekonzepte zum Umgang mit personenbezogenen Daten durch Administratoren verwiesen wird.

Auch die normalen E-Mail-Angebote einiger Anbieter wurden im Datenschutz verbessert: So finden z. B. mittlerweile zwischen den E-Mail-Servern des Mailverbunds von GMX, WEB.DE, freenet.de und T-Online ausschließlich verschlüsselte Datenübertragungen statt. Mit dem Siegel „E-Mail Made in Germany“ soll damit geworben werden, dass das Datenschutzrecht in Deutschland eingehalten wird und die Daten auch hier gespeichert werden. Wenn sich der Initiative noch mehr Anbieter anschließen würden, wäre das zumindest zu begrüßen, auch wenn es sich dabei nur um eine Transportverschlüsselung handelt. Wie bei De-Mail wird eine Ende-zu-Ende-Verschlüsselung nicht angeboten. Hier muss jeder Nutzer wieder selbst aktiv werden, wenn eine solche Ende-zu-Ende-Verschlüsselung eingerichtet werden soll. Wie die bisherige Praxis aber zeigt, ist der normale Nutzer mit der Verschlüsselung seiner E-Mails überfordert und deshalb erfolgt der E-Mail-Verkehr weitestgehend unverschlüsselt.

Der Landesbeauftragte weist darauf hin, dass personenbezogene Daten mit besonderem Schutzbedarf, wie z. B. medizinische Daten, durch den Versender ggf. mit zusätzlichen Schutzmaßnahmen gesichert übertragen werden müssen oder andernfalls nicht übertragen werden dürfen. Diese Absicherung und vorab die Prüfung, ob eine solche notwendig ist, muss der Datenversender vornehmen. Diese Sichtweise ist mittlerweile auch durch einen Beschluss des Bundesgerichtshofs vom 26. Februar 2013 bestätigt worden (ZD 2013, 273). Behörden dürfen keinen ungesicherten E-Mail-Versand verlangen. Davon sind nicht nur „Betriebs- oder Geschäftsgeheimnisse“, sondern auch alle anderen Daten, hier „unternehmensinterne Daten“, erfasst, die nicht „über eine ungesicherte E-Mail-Verbindung an die Behörde“ übermittelt werden dürfen, sofern der Absender dies nicht möchte. Wenn eine Behörde oder ein Unternehmen keine verschlüsselten Übertragungswege anbietet, kann eine unverschlüsselte Kommunikation via E-Mail nicht gefordert werden.

Am 25. Juli 2013 wurde das E-Government-Gesetz (EGovG) vom Bundestag beschlossen (BGBl. I S. 2749), welches zumindest für Bundesbehörden klarstellt, dass diese einen Zugang für elektronische Dokumente, insbesondere auch solche, die mit einer qualifizierten Signatur versehen sind, einrichten müssen. Ebenso müssen Bundesbehörden einen De-Mail-Zugang anbieten, der aber wohl zentral bereitgestellt werden wird. Damit ist der Anfang gemacht und Bundesbehörden müssen sich mit Themen wie PKI, eID, Zertifikaten, Verschlüsselung und Signatur beschäftigen und teilweise auch entsprechende Zugänge einrichten. In diesem Zusammenhang regt der Landesbeauftragte ein E-Government-Gesetz für das Land Sachsen-Anhalt an (Nr. 4.2).

Des Weiteren regt der Landesbeauftragte, informiert durch Rundschreiben Nr. 388 des Landkreistages vom 15. Juli 2013, an, die Domain de-mail.de mit entsprechenden landes- und behördenspezifischen Subdomains zu nutzen. Auch Kommunen können entsprechende Adressen für die eigene Nutzung reservieren lassen. Damit ein Wildwuchs oder Abhandenkommen solcher Subdomains verhindert wird, wurden die Staatskanzlei und das

Ministerium für Finanzen als dafür zuständige Stellen angesprochen, um eine zentrale Koordinierung zu veranlassen.

Auch der Landesbeauftragte erwägt, einen De-Mail-Zugang anzubieten, um den Bürgerinnen und Bürgern eine weitere und bessere Möglichkeit zur Kontaktaufnahme und Kommunikation zu ermöglichen. Es hat sich bisher gezeigt, dass meistens die unsichere E-Mail-Kommunikation ohne Verschlüsselung gewählt wird, obwohl der Landesbeauftragte seinerseits die verschlüsselte E-Mail-Kommunikation mittels öffentlichem PGP-Schlüssel bzw. X.509-Zertifikaten ermöglicht.

4.6 Datenschutzmanagement

Im X. Tätigkeitsbericht (Nr. 2.1) hat der Landesbeauftragte die Initiative zum Datenschutzmanagement in Behörden vorgestellt und auf die Broschüre auf der Homepage hingewiesen. Die Reihe der Besuche in den Kommunen wurde erfolgreich fortgesetzt. Die Behördenleitungen konnten ebenso wie die Mitarbeiterinnen und Mitarbeiter in datenschutzrechtlichen Fragen sensibilisiert werden. Auch gab es Gelegenheit, in verschiedenen Themenbereichen Verbesserungen vorzuschlagen. In technisch-organisatorischer Hinsicht konnten beispielsweise die Verträge zur Schriftgutentsorgung, die Aufnahme der behördlichen Datenschutzbeauftragten in das Organigramm, das Verfahrensverzeichnis und der rechtskonforme Internetauftritt angesprochen werden. Im Personalwesen wurden u. a. der Umlauf der Krankmeldungen und die Aufbewahrung von Einstellungstests und Bewerbungsunterlagen kritisch hinterfragt. Neben Einzelaspekten des Melde- und Ausweiswesens wurden im Bereich der Ratsinformationssysteme u. a. Zugriffsregelungen, die Veröffentlichung von Bürgeranfragen und grundlegend die Datensparsamkeit und Datenvermeidung thematisiert.

Auch im nicht-öffentlichen Bereich ist ein angemessenes Datenschutzmanagement geboten. Der Landtag von Sachsen-Anhalt hat dies in seiner Entschließung zur Fortentwicklung des Datenschutzes vom 19. Oktober 2012 (LT-Drs. 6/1545) zum Ausdruck gebracht. Für den Bedarf der Wirtschaftsunternehmen sind danach Konzepte und Maßnahmen zu entwickeln, die Informationen zu einem modernen Datenschutz und einer risikoadäquaten Informationssicherheit und die Wahrnehmung eines Datenschutzmanagements als Führungsaufgabe unterstützen. Der Landesbeauftragte beteiligt sich an den Aufgaben u. a. mit Empfehlungen, Beratungen und Vorträgen.

Datenschutz ist auch in Wirtschaftsunternehmen eine **Führungsaufgabe**. Dabei ist zunächst die schlichte Einhaltung der gesetzlichen Vorgaben (insbesondere des BDSG) zu sichern. Auch im Rahmen der wirtschaftlichen Entfaltungsfreiheit ist der angemessene Schutz der Persönlichkeitsrechte der von Datenverarbeitung Betroffenen zu berücksichtigen. Im Rahmen der Gesetze ist durch entsprechende Selbstregulierung hierfür zu sorgen. Die notwendigen Vorgaben zur Umsetzung obliegen der Unternehmensleitung. Von dort sollte eine angemessene Datenschutzkultur

ausgehen, vorgegeben und vorgelebt werden. Letztlich fördert dies Vertrauen und spricht damit auch als Werbung für das Unternehmen.

Steuerungsinstrumente wären u. a. Handlungsanweisungen und Betriebsvereinbarungen. Mitarbeiter können geschult werden. Technisch-organisatorische Maßnahmen der Datensicherheit sind zu treffen. Inhaltlich beginnt es bei der Ausgestaltung der Technik (z. B. durch privacy by design oder privacy by default). Eine interne oder externe Kontrolle sollte eingerichtet werden. Die Vorgaben zur Bestellung betrieblicher Datenschutzbeauftragter sind zu beachten (siehe dazu § 4f BDSG; vgl. zu Mindestanforderungen an Fachkunde und Zuverlässigkeit den Beschluss des Düsseldorfer Kreises vom 24./25. November 2010; die wichtigsten Aufgaben sind in § 4g BDSG aufgeführt). Weiter ist ein angemessener Beschäftigtendatenschutz notwendig. Nicht zuletzt ist die sachdienliche und effiziente Wahrnehmung der Betroffenenrechte der Unternehmenskunden zu gewährleisten.

Der Landesbeauftragte beabsichtigt, auch für den Bereich der Unternehmen eine Broschüre herauszugeben.

4.7 Cloud-Computing – weitere Entwicklung

Über die Grundlagen des Cloud-Computing, dessen Dienstarten und Organisationsformen, hatte der Landesbeauftrage im seinem X. Tätigkeitsbericht (Nr. 14.1) informiert. Das BSI hat in seinen am 10. Mai 2011 im Rahmen des 12. Deutschen IT-Sicherheitskongresses veröffentlichten Sicherheitsempfehlungen für Cloud-Computing-Dienste Mindestanforderungen an die Informationssicherheit zur Minimierung der Risiken bei der Nutzung von Cloud-Lösungen zusammengestellt. Bis Ende 2013 werden diese Eckpunkte als Bausteine Cloud-Management, Cloud-Nutzung, Web-Services und Cloud-Storage in die IT-Grundschutzkataloge einfließen und bilden damit eine geeignete Grundlage, um Cloud-Lösungen nach ISO 27001 auf Basis von IT-Grundschutz zertifizieren zu können.

Durch die Arbeitskreise Technik und Medien wurde eine Orientierungshilfe zum Umgang mit Cloud-Computing erarbeitet, welche auf der 82. Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen wurde. Die Orientierungshilfe mit Erscheinungsdatum 26. September 2011 informiert über Mindestanforderungen an Cloud-Anbieter, die ein datenschutzkonformes Einsatzszenario erst möglich machen können. So müssen Cloud-Anbieter detaillierte Informationen zur technologischen Umsetzung und rechtlichen Rahmenbedingungen ihres Angebotes transparent darstellen, damit überhaupt eine Einschätzung über die datenschutzkonforme Nutzung angebotener Dienste und somit eine Auswahl der nutzbaren Dienste getroffen werden kann. Dazu gehören auch Informationen zu getroffenen Sicherheitsmaßnahmen und zu geltendem bzw. anzuwendendem Recht bei Diensten, die vollständig oder teilweise außerhalb der Mitgliedstaaten der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum bereitgestellt werden. Außerdem müssen bei Zustandekommen eines Nutzungsvertrages ein-

deutige Regelungen zu Methoden der Übermittlung und Datenverarbeitung, zum Ort, an dem die Datenverarbeitung physisch stattfindet, und zu Bedingungen, unter denen ein dynamischer oder geplanter Ortswechsel der genutzten Ressourcen vorgesehen ist, getroffen werden. Umsetzung und Einhaltung konkreter Sicherheitsmaßnahmen zum Schutz der Daten müssen durch den Cloud-Anwender gefordert und vom Cloud-Anbieter geleistet werden. Der Cloud-Anbieter sollte nach Möglichkeit Zertifizierungen zur Sicherheitsinfrastruktur, Portabilität und Interoperabilität nachweisen, um die Auftragserfüllung garantieren zu können.

Die Artikel-29-Datenschutzgruppe hat mit dem Arbeitspapier WP 196 am 1. Juli 2012 „Stellungnahme 05/2012 zum Cloud Computing“ eine Auseinandersetzung mit den Herausforderungen des Cloud-Computing aus datenschutzrechtlicher Sicht veröffentlicht, die auch die Übertragung von Daten an Cloud-Anbieter außerhalb der Mitgliedstaaten der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum betrachtet. Hier wird der Cloud-Anbieter ebenfalls als Auftragsdatenverarbeiter betrachtet und der Cloud-Anwender als verantwortliche Stelle. Es muss also auch zur Einhaltung der EU-Datenschutzrichtlinie 95/46/EG eine vertragliche Absicherung zwischen Auftraggeber und Auftragnehmer der Datenverarbeitung existieren. Werden durch den Cloud-Anbieter Subunternehmen eingeschaltet, so muss dies im Einvernehmen mit dem Auftraggeber geschehen, die Subunternehmer müssen ihm also bekannt sein, und auch die Subunternehmer haben Verträge einzuhalten, die das Datenschutzinteresse des Cloud-Anwenders wiederspiegeln. Außerdem müssen in den Verträgen zur Auftragsdatenverarbeitung der Ort der physikalischen Datenverarbeitung, technisch organisatorische Maßnahmen zur Gewährleistung der Datensicherheit, anzuwendende Löschtechniken, Dauer, Ziele und Gegenstand des Dienstes sowie Service Level und Vertragsstrafen festgelegt sein. All dies geht weitestgehend einher mit den Regelungen des BDSG. Weitergehend sind lediglich die Empfehlungen der Europäischen Kommission, dass der Cloud-Anwender seine Kunden und Beschäftigten darüber informiert, dass er ihre personenbezogenen Daten an einen Cloud-Anbieter übergibt, und dass der Cloud-Anbieter und seine Subunternehmer dem Cloud-Anwender in Person bekannt sein sollten.

Der Düsseldorfer Kreis hatte schon im April 2010 zur Nutzung von Cloud-Diensten für Datenverarbeitung in Ländern, die Safe Harbor-zertifiziert sind, wie z. B. die USA, zusätzliche Maßnahmen in einem Beschluss formuliert. Zunächst muss durch den Cloud-Anwender aufgeklärt werden, ob die Safe Harbor-Zertifizierung des Staates, in dem der Cloud-Anbieter seinen Hauptsitz hat und wo die Datenverarbeitung physikalisch stattfindet, zum Zeitpunkt der Vertragsschließung Bestand hat. Der Cloud-Anwender soll sich ebenfalls vom Anbieter nachweisen lassen, wie er seinen Informationspflichten gegenüber den von der Datenverarbeitung betroffenen Personen nachkommen und welche Mittel er einsetzen wird, um die Weitergabe der Daten einzuschränken. Der Anwender soll die zuvor genannten Maßnahmen dokumentieren, um Sie seiner zuständigen Aufsichtsbehörde auf Nachfrage vorlegen zu können.

Die Verarbeitung personenbezogener Daten bei einem Cloud-Anbieter ist in jedem Falle als Auftragsdatenverarbeitung zu behandeln. Eine pauschale Nutzung von Cloud-Diensten zur Datenverarbeitung ohne konkrete vertragliche Regelungen kann den Anforderungen an den Datenschutz nicht gerecht werden. Kritisch zu betrachten ist der Zugriff ausländischer Geheimdienste und Regierungsorganisationen auf die im Ausland verarbeiteten Daten. Trotz vertraglicher Regelungen zwischen den Entitäten der Datenverarbeitung und trotz Safe-Harbor-Zertifizierung besteht die Gefahr, dass nationales Recht in anderen Ländern erlaubt, ausländische personenbezogene Daten von den verarbeitenden Unternehmen zur Übermittlung anzufordern, zu verarbeiten und zu nutzen, wie zuletzt in Bezug auf die USA mit Veröffentlichung von Informationen zum Projekt PRISM bekannt geworden. Daher ist es empfehlenswert, soweit wie möglich Cloud-Dienste bei Anbietern und deren Subunternehmen innerhalb Deutschlands bzw. innerhalb der Mitgliedstaaten der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zu buchen, sodass sowohl Standort der Datenverarbeitung als auch anzuwendendes Recht mit dem BDSG vereinbar sind.

Ein Entwurf zur Änderung des Datenschutzgesetzes Sachsen-Anhalt sieht im Rahmen der Auftragsdatenverarbeitung des § 8 DSG LSA Erleichterungen für die Beauftragung von ausschließlich Speicherdienstleistungen dahingehend vor, dass im Falle der vollständigen und sicheren Verschlüsselung der Daten durch die verantwortliche Stelle im Vorfeld der Übertragung nicht alle durch das Gesetz geforderten vertraglichen Regelungen und Kontrollen (§ 8 Abs. 2 bis 6 DSG LSA) umgesetzt werden müssen. Dadurch würde zumindest die Speicherung verschlüsselter Daten bei Cloud-Anbietern aus rechtlicher Sicht erleichtert werden.

4.8 Vernichtung von Datenträgern – neue DIN 66399

Ein ständig wiederkehrendes Thema sind Anfragen beim Landesbeauftragten zu Anforderungen an die Vernichtung von Schriftgut. Allgemeine Maßgaben hierfür sieht das DSG LSA in § 16 vor. Bei der Vernichtung von Schriftgut handelt es sich um die letzte Datenverarbeitungsphase, das Löschen von personenbezogenen Daten. Das Löschen von personenbezogenen Daten, bei Schriftgut das Vernichten, hat zeitnah und in besonderen Fällen unverzüglich (z. B. noch am gleichen Tag) zu erfolgen. Generell sollte zu vernichtendes Schriftgut mit personenbezogenen Daten von sonstigem Papierabfall getrennt und, wenn nötig, in sicher verschlossenen Behältnissen bis zu seiner Vernichtung gesammelt werden.

Grundlage für die Vernichtung von Datenträgern mit personenbezogenen Daten war bisher die DIN 32757 vom Oktober 1985. Diese beinhaltet fünf Sicherheitsstufen, in denen die Restpartikelgröße sowie Toleranzbereiche festgelegt waren. Diese DIN wurde im Oktober 1993 überarbeitet und gab Anlass für den Landesbeauftragten, in seinem damaligen II. Tätigkeitsbericht (Nr. 13.5.6) Hinweise zur Aktenvernichtung zu geben. Bei der Anschaffung eigener Aktenschredder bei öffentlichen Stellen und beim Abschluss von Verträgen zur Aktenvernichtung im Rahmen der Auf-

tragsdatenverarbeitung (§ 8 DSG LSA) war es deshalb bisher erforderlich, Technik zu beschaffen bzw. vertraglich sicherzustellen, dass eine Vernichtung mindestens nach DIN 32757 Sicherheitsstufe 3 erfolgte. Diese DIN war lange Zeit der grundlegende Standard für die Vernichtung von Schriftgut mit vertraulichen, personenbezogenen oder sensiblen Daten.

Im Oktober 2012 wurde die bisherige DIN 32757 durch die neue DIN 66399 (Büro- und Datentechnik – Vernichten von Datenträgern) ersetzt. Diese neue DIN 66399 umfasst drei Teile (DIN 66399-1: Teil 1: Grundlagen und Begriffe; DIN 66399-2: Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern; DIN SPEC 66399-3: Teil 3: Prozess der Datenträgervernichtung).

Neu sind hierbei im Teil 1 (DIN 66399-1) die Einführung von Schutzklassen, d. h. die Klassifizierung von Daten nach ihrem Schutzbedarf, und die Unterteilung in nunmehr sieben Sicherheitsstufen. Bei den Schutzklassen lehnt sich die neue DIN an die Definition der Schutzbedarfskategorien des BSI an (BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise). Die Einteilung erfolgt in drei Schutzklassen: 1 (normaler Schutzbedarf), 2 (hoher Schutzbedarf) und 3 (sehr hoher Schutzbedarf).

Teil 2 (DIN 66399-2) umfasst die Anforderungen an Maschinen zur sicheren Vernichtung von Datenträgern in Abhängigkeit von der jeweiligen Sicherheitsstufe. Sie legt für jede Datenträger-Kategorie jeweils sieben Sicherheitsstufen fest. Neben dem klassischen Datenträger Papier werden hier auch für weitere Datenträger wie Mikrofilme, optische Datenträger (CD, DVD usw.), magnetische Datenträger (z. B. Disketten, Magnetstreifenkarten), elektronische Datenträger (z. B. USB-Sticks, Chipkarten, Flash-Speicher, SSD) und Festplatten die maximale Materialteilchenfläche in Abhängigkeit von der Sicherheitsstufe festgeschrieben. Hierbei gilt: Je höher die Sicherheitsstufe, desto kleiner die Material- bzw. Partikelgröße des geschredderten Materials und umso sicherer die Vernichtung der Daten.

Teil 3 (DIN SPEC 66399-3 als Vornorm) ist das Ergebnis eines Vornorm-Verfahrens und beschreibt Prozessketten der Datenträgervernichtung in drei Varianten:

- Variante 1 – Datenträgervernichtung durch die verantwortliche Stelle direkt,
- Variante 2 – Datenträgervernichtung durch Dienstleister vor Ort,
- Variante 3 – Datenträgervernichtung extern durch Dienstleister.

Erstmals wird damit in einer Norm die Vernichtung von Datenträgern als ein Prozess aufgefasst, der einer Risikobetrachtung unterzogen wird, in einzelne Prozessabschnitte unterteilt wird und für den danach Prozesskriterien für Bereiche wie Personal, Organisation, Sammeln, Transport, Lagerung, Vernichtung sowie Infrastruktur des Dienstleisters festgelegt werden. Damit wäre es der verantwortlichen Stelle (Auftraggeber) möglich,

sich von der Prozesssicherheit des Dienstleisters zu überzeugen und dies auch regelmäßig zu prüfen. In einem Audit durch akkreditierte Unternehmen beim Dienstleister vor Ort könnten der Prozessablauf und die einzelnen Prozessschritte anhand der Vorgaben dieser neuen DIN geprüft und durch ein entsprechendes Zertifikat bestätigt werden. Letztendlich bleibt für den Gesamtprozess der Datenträgervernichtung und die Einhaltung der erforderlichen technischen und organisatorischen Sicherungsmaßnahmen gem. § 8 Abs. 1 DSG LSA der Auftraggeber verantwortlich.

Grundsätzlich sollte deshalb bei der Vernichtung von Datenträgern mit Personenbezug, trotz der Unterteilung in verschiedene Datenträger-Kategorien, mindestens die Einstufung in Schutzklasse 2 und die Vernichtung mindestens nach Sicherheitsstufe 3 erfolgen. Im Einzelfall kann natürlich auch die Einstufung in Schutzklasse 3 ab Sicherheitsstufe 4 erforderlich sein, wenn es sich z. B. um sehr sensible personenbezogene Daten oder personenbezogene Daten besonderer Art (§ 2 Abs. 1 Satz 2 DSG LSA) handelt.

Auch wenn der Landesbeauftragte seit 1. Oktober 2011 die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich inne hat, besteht weiterhin die Verpflichtung, in Verträgen zur Auftragsdatenverarbeitung mit Auftragnehmern, für die das DSG LSA keine Anwendung findet, die Einhaltung des DSG LSA durch den Auftragnehmer und die Kontrollrechte des Landesbeauftragten gem. § 8 Abs. 6 DSG LSA vertraglich zu vereinbaren. Der private Auftragnehmer einer öffentlichen Stelle, für den das BDSG einschlägig ist, muss sich den Kontrollrechten gemäß DSG LSA unterwerfen, denn als Auftragnehmer einer öffentlichen Stelle des Landes sind auch durch ihn die Vorschriften zu erfüllen, die für seinen Auftraggeber Geltung besitzen.

Der Landesbeauftragte empfiehlt deshalb, beim Abschluss neuer Verträge zur Datenträgervernichtung die neue DIN 66399 zu berücksichtigen und seinen Empfehlungen zur Anwendung zu folgen. Bestehende Verträge sind zu überprüfen und entsprechend anzupassen. Die neue DIN 66399 sollte ebenfalls bei der Beschaffung von Aktenschreddern durch öffentliche Stellen selbst Beachtung finden.

Der Landesbeauftragte wird die Beachtung und Umsetzung der DIN 66399 bei seinen Kontrollen im öffentlichen wie im nicht-öffentlichen Bereich entsprechend berücksichtigen.

4.9 Mobile Computing – Datenschutz bei „Bring Your Own Device“

In seinem X. Tätigkeitsbericht (Nr. 14.3) äußerte sich der Landesbeauftrage zum Thema Mobile Computing, indem er die aktuellen Entwicklungen im Bereich Smartphones und Smartphone-Apps darstellte. Der geschäftliche Einsatz von Geräten aus dem Mobile Computing, die ursprünglich für den privaten Gebrauch entwickelt wurden, wird als Consumerisation bezeichnet. „Bring Your Own Device“ (BYOD) erweitert diesen Begriff dadurch, dass Beschäftigte in Absprache mit dem Arbeitgeber ihre privaten mobilen Endgeräte (Smartphones, Tablets, Notebooks) zur Durchführung

ihrer beruflichen Tätigkeiten verwenden dürfen oder sollen. Hierin finden sich viele Herausforderungen für die IT-Abteilungen und Datenschutzbeauftragten, denn private Endverbrauchergeräte sind nicht vornehmlich für den geschäftlichen Gebrauch konzipiert. Es bedarf vielerlei Analysen und Anpassungen, um die Geräte sicher in das professionelle Arbeitsumfeld zu integrieren. Potentielle Gefahren ergeben sich aus den Kommunikationsmöglichkeiten und den Zugriffsrechten der mobilen Endgeräte. Die Geräte können über WLAN am Behörden- bzw. Unternehmensnetzwerk angebunden werden und gleichzeitig per UMTS oder LTE mit dem öffentlichen Mobilfunknetz und somit mit dem Internet verbunden sein. Die Geräte erfassen per GPS Lokalisationsdaten und können daraus Bewegungsprofile erstellen und diese Dritten zur Kenntnis geben. Außerdem haben die Besitzer oftmals nicht genügend Kontrolle über Speicherbereiche und Hintergrundkommunikation der Geräte. So können von Geräteherstellern oder App-Anbietern Nutzungsverhalten und personenbezogene Daten vom Endgerät abgerufen und von Dritten statistisch verarbeitet und zu Marketingzwecken weitergegeben werden. Umgekehrt besteht die Möglichkeit, dass Schadsoftware, die bei privater Nutzung auf das Gerät gelangt ist, auf dem Gerät aktiv wird, um Daten aus dem Behörden- bzw. Unternehmensnetzwerk abzurufen, oder über das Gerät in das Netzwerk der Institution eingeschleust wird, um dort aktiv zur werden.

Grundsätzlich sind vier Szenarien bei BYOD denkbar. Entweder der Beschäftigte bekommt über eine gesicherte Verbindung Zugang zu einem Internetdienst, der ihm die benötigten Daten und Anwendungen lediglich anzeigt. Die Daten befinden sich dann zu keinem Zeitpunkt auf dem Gerät des Beschäftigten und die Bedienung der Anwendungen erfolgt mittels Internetbrowser. Das Gerät muss hierfür nicht in das Behörden- bzw. Unternehmensnetzwerk eingebunden sein. Oder der Beschäftigte bekommt intern über WLAN oder extern über einen verschlüsselten VPN-Tunnel einen direkten Zugang zum Behörden- bzw. Unternehmensnetzwerk und kann innerhalb dieser Verbindung dedizierte Terminaldienste verwenden. Auch hier befinden sich die Daten nicht auf dem mobilen Endgerät und die Interaktionen erfolgen per Fernsteuerung. Die Verbindung erfolgt in ein Netzwerksegment, das für unsichere mobile Endgeräte bereitgestellt wird und nicht mit dem Kernnetzwerk der Behörde bzw. des Unternehmens verbunden ist. Eine weitere Möglichkeit besteht darin, dem Beschäftigten eine gesicherte Verbindung zum Netzwerk zu gewähren, jedoch die Daten, die an die Endgeräte übertragen werden, auf den Geräten in sog. Containern zu verwalten. Container sind spezielle Umgebungen, die in gesicherten Bereichen der Geräte operieren und deren Datenhaltung und Zugriffsrechtemechanismen strikt getrennt von allen anderen privaten Anwendungen und Speicherbereichen der Geräte ausgeführt werden. Dabei sollte die Umsetzung dieser Trennung von privaten und dienstlichen Bereichen möglichst auf Betriebssystemebene der Geräte stattfinden und die Daten auf den Geräten ausschließlich verschlüsselt abgespeicherten werden. Außerdem sollte es möglich sein, dass bei Verlust ein Gerät durch die IT-Abteilung per Fernsteuerung gesperrt und die dienstlichen Daten gelöscht werden können. Ein Szenario, in dem den Beschäftigten der Zugriff auf das Behörden- bzw. Unternehmensnetzwerk durch das private

mobile Endgerät ohne Einschränkungen ermöglicht wird, ist generell abzulehnen und abzustellen. Die verantwortliche Stelle könnte dadurch die Kontrolle über die personenbezogene Daten, die in ihrer Hoheit liegen, vollständig verlieren, da von dem Beschäftigten eine selbstständige allumfassende Umsetzung von Datensicherheit auf dem eigenen mobilen Endgerät nicht erwartet werden kann.

Obwohl die Beschäftigten bei BYOD ihre eigenen mobilen Endgeräte für dienstliche bzw. geschäftliche Zwecke nutzen, liegt die Verantwortung der Datenverarbeitung weiterhin beim Arbeitgeber. Das heißt, der Arbeitgeber muss, wenn er BYOD zulässt oder anordnet, dafür sorgen, dass durch entsprechende technische und organisatorische Maßnahmen Datenschutz und Datensicherheit gewährleistet sind. Das BSI hat ein Überblickspapier zum Thema BYOD erstellt. Dort findet sich ein erster Handlungsleitfaden zum Umgang mit mobilen Endgeräten, der sich an die IT-Abteilungen richtet. Dieser umfasst einen Maßnahmenkatalog, der sich in organisatorische, technische und infrastrukturelle Maßnahmen aufgliedert.

Aus *organisatorischer* Sicht ist beim Einsatz von privaten mobilen Endgeräten in einer Behörde bzw. in einem Unternehmen eine strategische Konzeption unerlässlich. Es muss zunächst festgelegt werden, wer zu welchem Zweck mit welcher Art von Gerät im Behörden- bzw. Unternehmensnetzwerk tätig sein soll und welche Daten aus der Institution genutzt werden sollen. Darüber hinaus muss erfasst werden, welche mobilen Betriebssysteme dabei zugelassen werden und welche bekannten Sicherheitslücken der Systeme und administrativen Einschränkungen für die Nutzer zum Tragen kommen könnten. So muss sichergestellt sein, dass insbesondere personenbezogene Daten, die durch private mobile Endgeräte verarbeitet werden, nicht unverschlüsselt auf den Geräten gespeichert und ohne die Kontrolle der Nutzer an Dritte übermittelt werden. Es ist im Vorfeld zu prüfen, ob die für den Einsatz geplanten Technologien im Zusammenspiel mit der Auswahl an Endgeräten die Sicherheitsziele erfüllen können. Es sollte für Lösch-, Sperr- und Ortungsfunktionen eine Meldestelle (Hotline oder Internetformular) und ein Bereitschaftsdienst eingerichtet werden, sodass Betroffene den Verlust eines Gerätes unverzüglich melden können und sofort Maßnahmen eingeleitet werden können. Zu beachten ist hierbei, dass die Maßnahmen Löschung, Sperrung und Ortung teilweise nur ausgeführt werden können, solange sich die SIM-Karte noch im Gerät befindet und das Gerät in einem Mobilfunknetz eingebucht ist. Daher sollten die Reaktionsfristen möglichst kurz gehalten werden. Da die Beschäftigten bei BYOD die Möglichkeit haben, dienstliche bzw. geschäftsinterne personenbezogene Daten auf privaten Datenträgern außerhalb der Behörde bzw. des Unternehmens zu transportieren, ist die Verpflichtung aller Mitarbeiter auf das Datengeheimnis und auf die Einhaltung der für den Einsatz von BYOD vereinbarten Regeln und Maßnahmen essentiell. Zugleich muss sich der Arbeitgeber bewusst sein, dass alle nicht-dienstlichen bzw. nicht-geschäftlichen Daten der Beschäftigten auf den mobilen Endgeräten ebenfalls dem Datenschutz unterliegen und damit bei Zugriffsrechtekonzepten entsprechend berücksichtigt werden müs-

sen, d. h. keine Lese- und Schreibzugriffe sowie keine Lösch- sowie Sperrmaßnahmen für diese privaten Daten.

Technische Maßnahmen können zum Teil durch spezielle Software oder komplexe Unternehmenslösungen für Mobile-Device-Management umgesetzt werden. Die Prinzipien Zugangsberechtigung, Protokollierung, Datenfilterung und Verschlüsselung werden serverseitig gesteuert und auf den Geräten angewendet. Es sollte dann je nach Schutzbedarf eine Internetzugriffslösung durch ein gesichertes Internetportal, eine Terminaldienstlösung mittels gesicherten Fernzugriffs oder eine Container-Lösung in Form einer auf dem Gerät installierten Anwendung umgesetzt werden. Eine spezielle aber sehr sichere Umsetzungsform ist die der Virtualisierung. Dabei befinden sich private Anwendungen mit ihren Daten und dienstliche Anwendungen mit ihren Daten jeweils in getrennten virtuellen Maschinen, die innerhalb des Endgerätes keinen Kontakt zueinander haben. Es existieren jedoch noch keine erprobten Produktivsysteme zu diesem Lösungsansatz, da eine Virtualisierung so tief in die Betriebssystemschicht eines Gerätes eingreift, dass die Garantie für das Gerät verfallen würde oder die Lösung aufgrund der Architektur des Gerätes schlichtweg nicht realisierbar ist. Bei allen vorgenannten Szenarien ist auf den Einsatz eines Antivirenprogramms (auch Virenscanner oder Virenschutzsoftware bezeichnet) und auf das regelmäßige Einspielen der neusten Betriebssystem-Patches zu achten. Die Aktualisierung sollte so weit wie möglich automatisiert werden.

Infrastrukturelle Maßnahmen betreffen die Anbindung der mobilen Endgeräte an das Netzwerk der Institution. Diese sollte immer transportverschlüsselt sein. Außerdem sollten sowohl die mobilen Endgeräte als auch die Server, die Dienste für BYOD bereitstellen, in gesonderten Netzsegmenten, die durch eine Firewall von der internen und zentralen Serverarchitektur abgeschottet sind, untergebracht sein. Es sollte ebenfalls ein abgetrenntes Quarantäne-Netzsegment geben, in welchem Geräte mit Sicherheitslücken für Wartungs- und Updatezugriffe durch die IT-Abteilung eingebunden werden können.

Aus rechtlicher Sicht kommen verschiedene Normen zur Anwendung. Zum einen ist es Beschäftigten untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (§ 5 DSG LSA, § 5 BDSG). Daher sollten Beschäftigte immer nach einer entsprechenden Schulung auf das Datengeheimnis verpflichtet werden. Außerdem sollte der besondere Umgang mit Endgeräten, Daten und Sicherheitsrichtlinien beim Einsatz von BYOD in einer Betriebsvereinbarung (§ 77 BetrVG) zwischen Arbeitgeber und Betriebsrat unter Mitarbeit der IT-Abteilung geregelt werden. So kann rechtlich sichergestellt werden, dass die Beschäftigten die verabredeten Regeln und vorgegebenen Sicherheitseinstellungen kennen und sich bewusst sind, dass sie diese nicht umgehen dürfen. Außerdem ist sicherzustellen, dass Regelungen zur Bereinigung der Geräte für den Fall existieren, dass Mitarbeiter ihre mobilen Endgeräte verlieren oder zur Reparatur geben. Das Gleiche gilt für den Fall, dass Mitarbeiter die Behörde bzw. das Unternehmen verlassen oder in einen anderen Tätigkeitsbereich innerhalb der Institution wechseln. Die Mitarbeiter sollten verpflichtet wer-

den, die automatische Aktualisierung des Antivirenschutzprogramms und des Betriebssystems nicht zu verhindern, und die Geräte nicht zu „rooten“ oder einen „Jailbreak“ auszuführen. Der Begriff „root“ kommt aus dem Unix-Umfeld und bezeichnet ein Nutzer-Konto, mit allen Zugriffs- und Schreibrechten auf das Betriebssystem. Als „Jailbreak“ bezeichnet man einen Vorgang, der das Apple-Betriebssystem des iPhones (iOS) für Lese- und Schreibvorgänge zugänglich macht. Andererseits muss das Einverständnis der Beschäftigten eingeholt werden, wenn durch die IT-Abteilung spezielle Programme installiert, automatisierte Scans der Geräte durchgeführt und die Geräte in kompromittierenden Situationen gesperrt oder deren Inhalte gelöscht werden sollen.

Der Beschäftigte kann sich zum Schutz seiner privaten Daten auf dem mitgebrachten Endgerät auf BDSG und StGB stützen. So ist jegliche Erhebung und Nutzung personenbezogener Daten von Beschäftigen, sofern sie nicht zur Durchführung des Beschäftigungsverhältnisses benötigt werden, was wohl auf alle privaten Dateien auf dem Endgerät des Beschäftigten zutreffen dürfte, verboten (§ 32 BDSG). Außerdem wird mit Freiheits- oder Geldstrafe bestraft, wer sich Zugang zu Daten, die nicht für Ihn bestimmt sind verschafft (§ 202a StGB). Zusätzlich wird das Abfangen von Daten, die nicht für Dritte bestimmt sind, bestraft (§ 202b StGB). Erfasst werden hier alle Formen der elektronischen Übermittlung wie E-Mail, SMS und Telefon. Die Vorbereitung einer Straftat nach §§ 202a und 202b ist ebenfalls eine Straftat (§ 203c StGB). Grundsätzlich haftet das Unternehmen für Handlungen und Unterlassungen, die der Sorgfalt eines ordentlichen Geschäftsbetriebes widersprechen.

Unter Federführung des Bayerischen Landesamts für Datenschutzaufsicht erarbeiten die Landesbeauftragten gemeinsam eine Orientierungshilfe für Apps und App-Anbieter sowie einen Katalog zur Prüfung von Apps für die Aufsichtsbehörden, um zukünftig zum Thema Datenschutz von Smartphone-Apps gezielt beratend und prüfend tätig werden zu können.

4.10 IPv6

Im X. Tätigkeitsbericht des Landesbeauftragten wurden in Nr. 14.4 bereits die essentiellen Möglichkeiten für einen datenschutzgerechten Einsatz von IPv6 vorgestellt. Aus diesem Grunde wird hier nur die aktuelle Weiterentwicklung dargestellt.

Der Erfolg der flächendeckenden IPv6-Einführung hängt stark von den Umstellungen bei den Internet-Providern ab. Einige bieten bereits – nicht zuletzt gezwungen durch einen stetig zunehmenden IPv4-Adressmangel – IPv6-Zugänge an. Je mehr Nutzer IPv6 einsetzen wollen, desto mehr wird diesem Bedarf auch durch die Diensteanbieter entsprochen werden müssen, um den Bedarf zu befriedigen. Auch im Land Sachsen-Anhalt hängen Angebot und Nachfrage direkt zusammen. An der Herstellung der IPv6-Fähigkeit des Landesnetzes wird gearbeitet. Mittelfristig ist damit zu rechnen, dass IPv4 weiterhin funktionieren, aber auch das IPv6 zunehmend als Voraussetzung für Fachverfahren und Projekte gefordert werden wird

und damit bereitgestellt werden muss. Beispielsweise aktuelle Mobilfunktechnologien (LTE) sind ohne IPv6 kaum vorstellbar und nutzen bereits gezielt die dadurch neuen Möglichkeiten (Mobile IP).

Das Bundesministerium des Innern beantragte bereits 2009 IPv6-Adressen bei der RIPE NCC und erhielt einen weltweit eindeutigen Adressraum zur Nutzung übertragen. Die Adressen werden z. B. Behörden kostenfrei und zeitlich unbeschränkt zur Verfügung gestellt. Ihre Verwaltung auf der obersten Ebene erfolgt durch die LIR „de.government“. Die Länder verteilen die Adressblöcke für ihre Behörden durch eigene Sub-LIRs. Diese verwalten i. d. R. auch die Adressbereiche der zugehörigen Kommunen.

Der Landesverwaltung Sachsen-Anhalt steht die Umstellung auf IPv6 noch bevor. Aufgrund der internen IP-Struktur des Landesnetzes (ITN-LSA) besteht kein unmittelbarer Zeitdruck, jedoch darf auch hier der Anschluss nicht verpasst werden. Das Technische Polizeiamt (TPA), das Ministerium der Finanzen und das Landesrechenzentrum arbeiten hierbei eng zusammen. Unter anderem durch Teilnahme an der 2010 eingerichteten IPv6-Arbeitsgruppe (IPv6-AG) auf Bundesebene, die die in der öffentlichen Verwaltung vorhandenen IPv6-Kompetenzen bündeln und Vorschläge für die IPv6-Umsetzung erarbeiten soll, werden gezielt Kompetenzen erworben und ausgebaut.

Im Juli 2013 wurde mit Hilfe einer Consulting-Firma am IPv6-Adressrahmenkonzept für das Land Sachsen-Anhalt und den Anträgen für die Sub-LIR gearbeitet. Der Landesbeauftragte erwartet, dass diese Anforderungen bezüglich des datenschutzgerechten Einsatzes von IPv6 bei der Konzeption und dem Aufbau des neuen Landesnetzes (ITN-XT) sowie bei der Auswahl und Entscheidung für einen Betreiber Ende des Jahres 2013 und die Betreuung durch den neuen zentralen Dienstleister (Dataport) berücksichtigt werden.

Die Bundesstelle für Informationstechnik im Bundesverwaltungsamt stellt interessierten IPv6-Nutzern im Internet einen lesenswerten „IPv6 Migrationsleitfaden“ nicht nur „für die öffentliche Verwaltung“ bereit. Anhand von typischen Einsatz-Szenarien (mobiler Einzelarbeitsplatz, mittlere Behörde der öffentlichen Verwaltung, bis hin zum großen Rechenzentrum) werden detaillierte Hinweise zur Einführung von IPv6 gegeben.

Entsprechende Hinweise und Anforderungen für einen datenschutzgerechten Einsatz von IPv6 haben die Datenschutzbeauftragten des Bundes und der Länder bereits auf der 82. Konferenz mit der Entschließung vom 28. September 2011 (**Anlage 6**) und die Beauftragten für Datenschutz und für die Privatsphäre auf der 33. Internationalen Konferenz mit einer Entschließung vom 3. November 2011 (**Anlage 38**) gegeben. Die Entschließung vom 8. November 2012 der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (**Anlage 19**) wendete sich insbesondere an Provider und Hersteller von IPv6-Technik. Mit einer Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ (Stand: 26. Oktober 2012) wurden die Hinweise

und Forderungen aus dem Jahr 2011 präzisiert (siehe Homepage des Landesbeauftragten).

4.11 Kontaktformular im Landesportal – Teil II

Durch Anklicken eines auf fast jeder Seite des Landesportals www.sachsen-anhalt.de vorhandenen Service-Icons „Briefumschlag“ mit dem treffenden Titel „Kontakt“ besteht für die Nutzer die Möglichkeit, eine E-Mail an die Online-Redaktion der Staatskanzlei zu senden. Der Landesbeauftragte hatte jedoch in den zurückliegenden Jahren beobachtet, dass mit der zunehmenden Zahl der Besucher seiner Webseiten im Landesportal immer mehr Bürgerinnen und Bürger in der Annahme, direkt mit dem Landesbeauftragten zu kommunizieren, der Online-Redaktion des Landesportals in der Staatskanzlei ihre datenschutzrechtlichen Anliegen schilderten. Die Staatskanzlei leitete die an den Landesbeauftragten gerichteten „Irrläufer“ zwar flugs an ihn ebenso wie die vielen hundert an andere Behörden gerichtete Mitteilungen an diese weiter, trotzdem kam es fortwährend zu von den Nutzern unbemerkten Datenübermittlungen an eine unzuständige Stelle. Da die direkte Kontaktaufnahme des Landesbeauftragten mit der Staatskanzlei nicht zu einer wirklich geeigneten Abhilfe des Problems geführt hatte, berichtete er in seinem IX. Tätigkeitsbericht (vgl. Nr. 2.5) und im X. Tätigkeitsbericht (vgl. Nr. 14.8) der Öffentlichkeit darüber. Datenschutzrechtlich hilfreiche Änderungen wurden ihm daraufhin angekündigt, dann jedoch entweder nicht realisiert oder die Ankündigung gar zurückgezogen. Es blieb zunächst alles beim Alten, weiterhin wurden monatlich hunderte teils datenschutz- und steuerrechtlich relevante Irrläufer durch die Staatskanzlei an die richtigen Empfängerbehörden weitergeleitet – mit dem entsprechend hohen Arbeitsaufwand.

Im Februar 2013 kündigte der Landesbeauftragte der Staatskanzlei eine Kontrolle des Kontaktformularverfahrens an. Das brachte Bewegung in die Angelegenheit. Die Staatskanzlei gab als für das Landesportal verantwortliche Stelle einem Dienstleister unverzüglich den Auftrag, eine Lösung für das Problem zu erarbeiten. Kurz nach Ende des Berichtszeitraumes wurde vom Dienstleister eine alternative Lösung unterbreitet. Die im Kontaktformular eingegebenen Mitteilungen werden direkt an die Behörde bzw. Stelle gesendet, von deren Seiten aus das Kontaktformular aufgerufen wurde. Die Lösung wurde, wie zwischen Staatskanzlei, Ministerium für Inneres und Sport und Landesbeauftragtem abgestimmt, realisiert. Allerdings zog die Staatskanzlei wenige Stunden nach der Inbetriebnahme der neuen Kontaktformular-Lösung ihre Zustimmung zum Verfahren ohne Begründung zurück und verlangte, den bisherigen Zustand wieder herzustellen.

Diese Verfahrensweise ist so nicht hinnehmbar. Der Landesbeauftragte erwartet, dass die Verantwortlichen in der Staatskanzlei die datenschutzgerechte Variante des „Kontaktformulars“ möglichst schnell wieder verfügbar machen.

4.12 Rundfunkfinanzierung – Sachstand und Umsetzung

Bereits in seinem X. Tätigkeitsbericht (Nr. 25.2) hat der Landesbeauftragte über die Neuregelung der Rundfunkfinanzierung durch den 15. Rundfunkänderungsstaatsvertrag und die damit verbundenen datenschutzrechtlichen Probleme berichtet.

Mit der Verabschiedung des Vierten Medienrechtsänderungsgesetzes im Dezember 2011 hat der Landtag von Sachsen-Anhalt dem 15. Rundfunkänderungsstaatsvertrag zugestimmt (GVBl. LSA S. 824). Allerdings hat der Landtag dazu einen Beschluss gefasst (LT-Drs. 6/566), in dem unter Punkt 4 neben der zeitnahen Evaluierung der datenschutzrechtlichen Regelungen weitere Forderungen aufgestellt werden, die u. a. hinsichtlich der Datensparsamkeit und Verhältnismäßigkeit auch die Bitte an die Landesregierung beinhalten, einen Verzicht auf den Adressabgleich mit nichtöffentlichen Stellen zu prüfen.

Aufgrund der datenschutzrechtlichen Probleme, die von den Landesdatenschutzbeauftragten im Rahmen von Anhörungen in verschiedenen Landtagen vorgetragen wurden, fand am 6. Oktober 2011 ein Gedankenaustausch statt, an dem sich Vertreter der Rundfunkanstalten, die Rundfunkdatenschutzbeauftragten und mehrere Landesdatenschutzbeauftragte beteiligten. Im Ergebnis wurden von ARD, ZDF und Deutschlandradio „Eckpunkte für eine Konkretisierung der datenschutzrechtlichen Regelungen im Vollzug des 15. Rundfunkänderungsstaatsvertrages“ formuliert, die wiederum in einen Satzungsentwurf gem. § 9 Abs. 2 Rundfunkbeitragsstaatsvertrag übernommen wurden.

Zur Ausgestaltung dieser Mustersatzung fanden ebenfalls Gespräche zwischen den Rundfunkdatenschutzbeauftragten und Vertretern der Landesbeauftragten für den Datenschutz statt. Obwohl eine Satzung nicht dazu geeignet ist, wichtige datenschutzrechtliche Regelungen anstelle eindeutiger und normenklarer Formulierungen im Staatsvertrag festzuschreiben, konnte im Ergebnis erreicht werden, dass z. B. die Befugnisse der „mit der Überprüfung der Einhaltung der Vorschriften des Rundfunkbeitragsstaatsvertrages beauftragten Dritten“ konkretisiert wurden.

Die Mustersatzung wurde von den Rundfunkanstalten übernommen, sodass der Rundfunkrat des Mitteldeutschen Rundfunks am 24. September 2012 die „Satzung des Mitteldeutschen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge“ beschlossen hat (MBl. LSA S. 621).

Der neue Rundfunkbeitragsstaatsvertrag trat zum 1. Januar 2013 in Kraft (Artikel 1 des 15. Rundfunkänderungsstaatsvertrages). Der bisherige Rundfunkgebührenstaatsvertrag wurde zeitgleich aufgehoben (Artikel 2 des 15. Rundfunkänderungsstaatsvertrages).

4.13 Neuregelung der Bestandsdatenauskunft

Mit seinem Beschluss vom 24. Januar 2012 (Az.: 1 BvR 1299/05; NJW 2012, 1419) hat das Bundesverfassungsgericht festgestellt, dass die Regelungen des § 113 Abs. 1 Satz 2 TKG zur Herausgabe von Zugangssicherungscodes (wie z. B. Passwörter zu E-Mail-Accounts, PIN oder PUK) an Ermittlungsbehörden und andere staatliche Stellen mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar sind und dem Grundsatz der Verhältnismäßigkeit widersprechen. Der Zugriff auf diese Daten sei in dem Umfang, wie ihn das TKG vorsehe, für eine effektive Aufgabenwahrnehmung der Behörden nicht erforderlich. Die Vorschrift stelle nicht hinreichend sicher, dass die Sicherheitsbehörden Auskünfte über die Zugangssicherungscodes nur dann verlangen dürfen, wenn die jeweils maßgeblichen gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Die Regelung wurde zugleich nur noch für eine Übergangsfrist bis zum 30. Juni 2013 für anwendbar erklärt.

§ 113 TKG hätte auch nicht für Auskünfte über den Inhaber einer dynamischen IP-Adresse herangezogen werden dürfen, da mit der Rückverfolgung einer dynamischen IP-Adresse ein Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis erfolge. In der Vergangenheit wurden in Deutschland tausende Nutzer von Filesharing-Programmen durch die Staatsanwaltschaften unter Berufung auf § 113 Abs. 1 Satz 1 TKG ermittelt und später von der Musik- oder Filmindustrie wegen Urheberrechtsverletzungen abgemahnt. Die auf diese Weise von den Providern verlangten Auskünfte sind demzufolge aufgrund einer verfassungswidrigen Interpretation des TKG erteilt worden.

Vom Gesetzgeber forderte das Bundesverfassungsgericht, § 113 TKG bis spätestens 30. Juni 2013 klarer zu fassen und im Gesetz deutlich zu machen, dass die Norm einen Grundrechtseingriff erlauben soll. Am 3. Mai 2013 hat der Bundesrat dem vom Bundestag am 21. März 2013 verabschiedeten Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft zugestimmt. Es ist zum 1. Juli 2013 in Kraft getreten (BGBl. I S. 1602).

Neben einigen datenschutzrechtlichen Verbesserungen wie dem bislang nicht existierenden Richtervorbehalt für die Abfrage von Zugangssicherungscodes durch Bundesbehörden sowie der neu eingeführten Benachrichtigungspflicht im Anschluss an Auskunftsverfahren, die die Zuordnung von dynamischen IP-Adressen oder Informationen über Zugangssicherungscodes zum Gegenstand hatten, gibt es nach wie vor Punkte, die aus datenschutzrechtlicher Sicht kritisch zu betrachten sind. So ist für die Auskunft über die Zuordnung von dynamischen IP-Adressen zu den Anschlussinhabern keine vorherige richterliche Genehmigung erforderlich. Obwohl das Bundesverfassungsgericht in seinem Beschluss vom 24. Januar 2012 explizit festgestellt hat, dass hierbei ein Eingriff in Art. 10 Abs. 1 GG vorliegt, diese Daten also unter das Fernmeldegeheimnis fallen, wurde auf einen Richtervorbehalt verzichtet.

Verfassungsrechtlich bedenklich ist die Bestandsdatenauskunft für die Verfolgung von Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung. Hier wäre eine Beschränkung auf schwerwiegende Straftaten und konkrete Gefahren zwingend erforderlich. Im Übrigen sind gem. § 46 Abs. 3 OWiG Auskunftsersuchen über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen, unzulässig.

Bereits am 1. Juli 2013, dem Tag des Inkrafttretens des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft, wurde eine Verfassungsbeschwerde beim Bundesverfassungsgericht eingereicht, da die Kläger in diesem Gesetz einen verfassungswidrigen Eingriff in ihr Recht auf informationelle Selbstbestimmung sehen. So bleibt abzuwarten, ob das Bundesverfassungsgericht auch dieses Mal die Verfassungswidrigkeit feststellen und den Gesetzgeber zu einer Nachbesserung verpflichten wird.

Zur Auskunftsbefugnis von Landesbehörden wird auf die Beiträge unter Nr. 5.1 und Nr. 8.4 verwiesen.

4.14 Leitfaden für eine datenschutzgerechte Speicherung von Verkehrsdaten

Im September 2011 kritisierte der Arbeitskreis Vorratsdatenspeicherung, ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern, Organisationen und Internet-Nutzern gegen die Vorratsdatenspeicherung, die Speicherpraxis bei Telekommunikationsdiensteanbietern. Obwohl für eingehende Gespräche in der Regel keine Gebühren anfallen, speichern die Telekommunikationsdiensteanbieter, wer wann von wem angerufen wurde. Auch bei Nutzung von Pauschaltarifen oder Flatrates wird gespeichert, wen man anruft oder wem man eine SMS sendet.

Datenschutzrechtlich besonders bedenklich ist die Speicherung von Ortungsdaten, da sich hierdurch umfassende Bewegungsprofile erstellen lassen. Jede Funkzelle, in die sich ein Mobiltelefon einbucht, wird von den Anbietern erfasst, auch wenn dies nicht für ortsgebundene Tarife notwendig ist. Dabei wird bis zu sechs Monate lang gespeichert, in welcher Funkzelle welcher Nutzer mit seinem Handy angerufen hat, angerufen wurde, SMS versandt oder empfangen hat.

Aus diesem Grund hat der Arbeitskreis Vorratsdatenspeicherung am 22. September 2011 bei der Bundesnetzagentur Anzeige gegen sechs Anbieter wegen ordnungswidriger Speicherung von Telekommunikationsverkehrsdaten erstattet.

Laut TKG dürfen die Telekommunikationsdiensteanbieter Verkehrsdaten zu Zwecken der Abrechnung (vgl. § 97 TKG) und der Störungsbeseitigung (vgl. § 100 TKG) speichern. Die im Gesetz gewählten Formulierungen sind allerdings unbestimmt und damit auslegungsfähig, da sie hauptsächlich auf den Begriff der Erforderlichkeit abstellen.

Um eine datenschutzgerechte und einheitliche Auslegung des TKG zu ermöglichen, haben die Bundesnetzagentur und der Bundesbeauftragte

für den Datenschutz und die Informationsfreiheit am 27. September 2012 in Hamburg einen gemeinsam entwickelten Leitfaden vorgestellt. Dieser „Leitfaden für eine datenschutzgerechte Speicherung von Verkehrsdaten“ soll den Anbietern von Telekommunikationsdiensten eine größere Rechtssicherheit bei der Speicherung von Verkehrsdaten verschaffen. Hierzu wird im Leitfaden klargestellt, welche betrieblichen Speicherfristen für Verkehrsdaten von den Aufsichtsbehörden im Regelfall als angemessen angesehen werden.

Für die Speicherung nicht abrechnungsrelevanter Verkehrsdaten zur Störungsbeseitigung oder Missbrauchserkennung hat sich die „Sieben-Tage-Regelung“ bewährt, da sowohl datenschutzrechtliche Belange als auch betriebliche Anforderungen der Netzbetreiber berücksichtigt werden (vgl. VIII. Tätigkeitsbericht, Nr. 23.2). Allerdings handelt es sich hierbei um eine Höchstfrist, d. h. die Daten sind vor Ablauf der sieben Tage zu löschen, wenn sie nicht mehr benötigt werden.

Die in § 97 Abs. 3 TKG festgelegte Höchstfrist von sechs Monaten für die Speicherung abrechnungsrelevanter Daten ist in der Praxis oft nicht erforderlich. Im Regelfall dürften drei Monate ausreichen, wobei begründete Ausnahmen möglich sind.

Der Arbeitskreis Vorratsdatenspeicherung kritisierte die fehlende Beteiligung von Verbraucher- und Bürgerrechtsverbänden bei der Erarbeitung des Leitfadens. Außerdem hält er die vorgeschlagenen Speicherfristen für zu weitreichend.

4.15 E-Privacy-Richtline

Bereits in seinem X. Tätigkeitsbericht (Nr. 25.6) hat der Landesbeauftragte über das vom EU-Parlament beschlossene Richtlinienpaket zur Novellierung des Regulierungsrahmens für Telekommunikationsnetze berichtet. Durch die EU-Richtlinie 2009/136/EG wurden einige Regelungen der E-Privacy-Richtlinie 2002/58/EG geändert, so u. a. Artikel 5 Abs. 3, der die Anforderungen an die Verwendung von Cookies verschärft. Deshalb wird die Richtlinie 2009/136/EG auch als sog. „Cookie-Richtlinie“ bezeichnet.

Cookies, die für die Erbringung eines Dienstes nicht erforderlich sind, dürfen nur noch dann verwendet werden, wenn der Nutzer vorher darin eingewilligt hat. Das gilt nicht für Cookies, deren alleiniger Zweck die Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist, sowie Cookies, die erforderlich sind, um den jeweiligen vom Nutzer ausdrücklich gewünschten Dienst zu erbringen.

Bislang gilt nach deutschem Recht die Widerspruchsregelung (Opt-Out), d. h. der Nutzer muss über die Verwendung von Cookies in der Datenschutzerklärung der Webseite informiert werden (§ 13 Abs. 1 Satz 2 TMG) und die Möglichkeit haben, dem Setzen des Cookies zu widersprechen (§ 15 Abs. 3 TMG). Bis 25. Mai 2011 hätte die „Cookie-Richtlinie“ in nationales Recht umgesetzt und anstelle der bisherigen Widerspruchs- eine Einwilligungsregelung (Opt-In) geschaffen werden müssen.

Der Bundesrat hat in seinem Beschluss (BR-Drs. 156/11) vom 17. Juni 2011 einen neuen § 13 Abs. 8 TMG vorgeschlagen, der auf eine explizite Umsetzung von Artikel 5 Abs. 3 der E-Privacy-Richtlinie 2002/58/EG abzielte. In der Stellungnahme der Bundesregierung zur BT-Drs. 17/6765 hat diese dazu lediglich erklärt, dass sie prüfen werde, wie durch eine Regelung im TMG Artikel 5 Absatz 3 der E-Privacy-Richtlinie umgesetzt werden könne. Die Bundesregierung werde dem Deutschen Bundestag – im Zuge der bereits im parlamentarischen Verfahren befindlichen Novellierung des TKG – hierzu eigene Vorschläge unterbreiten. Das ist bisher nicht geschehen.

Auf Initiative der SPD-Bundestagsfraktion wurde am 24. Januar 2012 ein weiterer Gesetzentwurf eingebracht, der eine Änderung des TMG zur Umsetzung von Artikel 5 Abs. 3 der E-Privacy-Richtlinie 2002/58/EG beinhaltete und den o. g. Vorschlag eines neuen § 13 Abs. 8 TMG aufgriff (BT-Drs. 17/8454). Dieser Gesetzentwurf wurde abgelehnt.

So stellt sich für Anbieter von Internetdiensten, die ihr Angebot rechtskonform gestalten wollen, die Frage, ob die „Cookie-Richtlinie“ unmittelbar Anwendung findet oder nicht. Die Auffassung, dass die E-Privacy-Richtlinie in Deutschland gilt, wird inzwischen von der Konferenz der Datenschutzbeauftragten und auch der Bundesregierung geteilt.

4.16 Netzneutralität

Die Deutsche Telekom AG hat für Neukunden oder Tarifwechsler, die seit dem 2. Mai 2013 einen Vertrag abgeschlossen haben, eine Volumenbegrenzung des Datenverkehrs ab 2016 angekündigt. Ursprünglich sollte beim Überschreiten des Vertragsvolumens die Geschwindigkeit auf 384 kbit/s abgesenkt werden, nunmehr wurde dieser Wert auf 2 Mbit/s erhöht. Damit liegt der neue Wert über der Grenze von 1 Mbit/s, den die Bundesregierung als Mindestrichtwert in der Breitbandstrategie empfiehlt.

Da die Deutsche Telekom AG jedoch die Nutzung eigener Angebote, die die Kunden gesondert bezahlen, auf das Volumen nicht anrechnen will, ist die Diskussion um das Thema Netzneutralität neu entflammt.

Netzneutralität bedeutet, dass alle Inhalte im Netz gleich behandelt bzw. Informationen gleich schnell übertragen und nicht aufgrund ihrer Qualität, ihrer Herkunft, ihrer Bestimmung, ihres Zwecks oder ihres Inhalts verlangsamt oder ganz blockiert werden. Aus Sicht des Endnutzers bedeutet Netzneutralität den freien Zugang zu Inhalten, Diensten und Anwendungen seiner Wahl. Aus Sicht des Anbieters von Inhalten, Diensten oder Anwendungen geht es um die uneingeschränkte Übermittlung der Informationen an den Endnutzer.

Steht ausreichend Bandbreite zur Verfügung, ist das Ziel der wertneutralen Datenübertragung leicht erfüllbar. Aufgrund begrenzter Ressourcen ist es für die Anbieter wichtig, Datenleitungen auszulasten und somit auch Datenströme zu priorisieren. Dies darf aber nicht zu Lasten der Endverbraucher gehen. Nur durch Gewährleisten der Netzneutralität wird der

gleichberechtigte Zugang zu allen Datenarten und damit eine datenschutzgerechte Datennutzung im Internet ermöglicht. Ohne den Grundsatz der Netzneutralität wäre z. B. die Verschlüsselung von Daten nur noch bedingt möglich, da verschlüsselte Daten anders behandelt werden könnten als unverschlüsselte. Verschlüsselung ist Stand der Technik und eine unverzichtbare technisch-organisatorische Maßnahme zur Gewährleistung der Vertraulichkeit von Datenübertragungen.

Der Begriff Netzneutralität ist gesetzlich nicht klar definiert, jedoch wird im § 41a TKG die Bundesregierung dazu ermächtigt, in einer Rechtsverordnung die grundsätzlichen Anforderungen an eine diskriminierungsfreie Datenübermittlung und den diskriminierungsfreien Zugang zu Inhalten und Anwendungen festzulegen, um eine willkürliche Verschlechterung von Diensten und eine ungerechtfertigte Behinderung des Datenverkehrs in den Netzen zu verhindern. Des Weiteren kann die Bundesnetzagentur in einer Technischen Richtlinie Einzelheiten über die Mindestanforderungen an die Dienstqualität durch Verfügung festlegen.

§ 41a TKG wurde durch das Gesetz zur Änderung telekommunikationsrechtlicher Regelungen eingefügt, welches am 10. Mai 2012 in Kraft trat. Weder von der Bundesregierung noch der Bundesnetzagentur wurden daraufhin Schritte bekannt, die vorgesehene Rechtsverordnung oder eine Technische Richtlinie zu erlassen.

Aufgrund der Drosselungspläne der Deutschen Telekom AG wurde im April 2013 beim Deutschen Bundestag eine Petition eingereicht, die ein Gesetz fordert, das Internetprovider verpflichtet, alle Datenpakete von Nutzern unabhängig von ihrem Inhalt und ihrer Herkunft gleich zu behandeln. Insbesondere sollen keine Inhalte, Dienste oder Dienstanbieter durch Provider benachteiligt, künstlich verlangsamt oder gar blockiert werden dürfen.
Insgesamt fand die Petition mehr als 77.000 Unterstützer, woraufhin sich der Petitionsausschuss des Deutschen Bundestags am 24. Juni 2013 in einer öffentlichen Sitzung mit dem Anliegen befasst hat. Sowohl die Opposition als auch die Koalition und die Bundesregierung waren sich darin einig, die Netzneutralität sichern zu wollen. Die zentrale Frage war, ob dies in einem Gesetz oder einer Verordnung geregelt werden soll. Während die Koalitionsfraktionen ebenso wie die Bundesregierung eine entsprechende Verordnung bevorzugten, plädierten SPD, Grüne und Linke für eine gesetzliche Festschreibung, wie es auch die Petition fordert.

Nachdem der erste Entwurf einer Netzneutralitätsverordnung nach § 41a Abs. 1 TKG, der bereits am 17. Juni 2013 vom Bundesministerium für Wirtschaft und Technologie veröffentlicht wurde, aufgrund massiver Kritik gescheitert war, wurde am 8. August 2013 ein neuer Verordnungsentwurf vorgestellt. Ein Beschluss des Bundeskabinetts ist vor den Neuwahlen im September nicht mehr erfolgt.

Womöglich wollte die Bundesregierung auf die Vorgaben der EU-Kommission warten, die ebenfalls die Netzneutralität gesetzlich verankern will. Mit einer entsprechenden Verordnung soll der EU-Telekommuni-

kationsmarkt reformiert und auch die Netzneutralität durchgesetzt werden. Dazu wurde am 12. September 2013 das Gesetzespaket „Vernetzter Kontinent“ (COM(2013) 627 final) vorgestellt, welches einen gesetzlichen Schutz für das offene Internet bieten soll. In der Verordnung steht kein explizites Datendiskriminierungsverbot, jedoch dürfen die Anbieter öffentlicher, elektronischer Kommunikation in einem offenen Internet Inhalte, Anwendungen oder Dienste weder blockieren, noch verlangsamen, verschlechtern oder diskriminieren. Nutzer sollen Zugang zu einem uneingeschränkten und offenen Internet, unabhängig von ihren vertraglich vereinbarten Kosten oder Geschwindigkeiten, erhalten. Dennoch können Unternehmen weiterhin Spezialdienste (z. B. IPTV, Video-on-Demand, Cloud-Anwendungen) mit zugesicherter Dienstqualität anbieten, solange dadurch die den anderen Kunden zugesagten Internetgeschwindigkeiten nicht eingeschränkt werden.

4.17 Videoüberwachungen

4.17.1 Allgemeines

Eine Erhebung personenbezogener Daten findet oft auch durch Videoüberwachung statt. Videoüberwachung ist ein Oberbegriff, der, so bestimmt es der auch für nicht-öffentliche Stellen geltende § 6b BDSG, für eine Beobachtung mit optisch-elektronischen Einrichtungen steht. Jedenfalls ist der Begriff „Videoüberwachung“ irreführend. Videoüberwachung durch optisch-elektronisches Beobachten findet nicht nur mittels herkömmlicher Videotechnik oder bei Webcams Anwendung. Digitale Fotokameras in den unterschiedlichsten Ausprägungen und selbst mit Kamera ausgestattete Mobiltelefone machen eine optisch-elektronische Beobachtung möglich. Dabei trügt der von der Öffentlichkeit gewonnene Eindruck keineswegs: Der Einsatz von Videoüberwachungen hat tatsächlich in den letzten Jahren stark zugenommen. Die Videoüberwachung ist i. d. R., auch wenn sie zum Massenphänomen geworden ist, als erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung zu werten. Dies beruht vor allem auch darauf, dass mit der Beobachtung zumeist eine Aufzeichnung des Beobachteten einhergeht.

Das DSG LSA, das ausschließlich für die öffentlichen Stellen des Landes gilt, normiert die dort „optisch-elektronische Beobachtung“ genannte Videoüberwachung in § 30.

Für die Polizei ist die Befugnis zur Videoüberwachung in § 16 SOG LSA spezialgesetzlich geregelt. Hinsichtlich der datenschutzrechtlichen Auswirkungen der Videoüberwachung durch die Polizei wird auf den IX. Tätigkeitsbericht (Nr. 18.6) und den X. Tätigkeitsbericht (Nr. 19.6) verwiesen. Hinsichtlich der tatsächlichen Durchführung von Videoüberwachungsmaßnahmen durch Polizeidienststellen des Landes Sachsen-Anhalt wird auf LT-Drs. 6/726 verwiesen.

4.17.2 Videoüberwachung im privaten Bereich

Der Landesbeauftragte erhält regelmäßig in erheblicher Anzahl Beschwerden über von Privatpersonen betriebene Videoüberwachungsanlagen. Ob für diese Fälle das BDSG überhaupt anwendbar ist, klärt sich mit der Beantwortung der Frage, wer bzw. was mit einer optisch-elektronischen Einrichtung, also einer Kamera, überwacht wird.

Videoüberwachung des eigenen Grundstücks

Aus den unterschiedlichsten Gründen überwachen Grundstückseigentümer ihren Besitz in zunehmendem Maße mittels Kameratechnik. Dies ist, soweit nicht z. B. Mieter oder Pächter betroffen sind, durchaus zulässig (vgl. Urteil des Bundesgerichtshofes vom 25. April 1995, Az. VI ZR 272/94, Rn 23, NJW 1995, 1955). Das BDSG ist in solchen Fällen nicht anwendbar, da die mit der Videoüberwachung möglicherweise einhergehende Datenerhebung und -verarbeitung für ausschließlich persönliche oder familiäre Tätigkeiten erfolgt (§ 1 Abs. 2 Nr. 3 BDSG). Der Landesbeauftragte ist für diese Fälle nicht zuständig.

Videoüberwachung öffentlich zugänglicher Räume

Die Rechtslage stellt sich anders dar, wenn öffentlich zugängliche Räume beobachtet bzw. überwacht oder im Fall der Überwachung des eigenen Grundstückes öffentlich zugängliche Räume mitüberwacht werden. Hier ist das BDSG anwendbar und damit die Zuständigkeit des Landesbeauftragten gegeben. Grundlage für die Beurteilung solcher Videoüberwachungen ist § 6b BDSG, der außer für öffentliche Stellen des Bundes auch für den nicht-öffentlichen Bereich gilt.

Zunächst muss geklärt werden, was unter öffentlich zugänglichen Räumen zu verstehen ist. Unter öffentlich zugänglichen Räumen sind nicht nur umbaute, sondern auch nicht umbaute Flächen zu verstehen, die nach dem erkennbaren Willen des Berechtigten den Zweck haben oder dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Zu den öffentlich zugänglichen Räumen zählen auch der Gehweg und die Straße vor einem Gebäude und die Zugänge zu diesem und den benachbarten Gebäuden, aber auch die Kundenbereiche von Kaufhäusern (siehe Nr. 4.17.3), Gastronomiebetrieben (siehe Nr. 4.17.4), Verkehrsunternehmen und öffentliche Grünanlagen. Ohne Relevanz sind im Übrigen die Eigentumsverhältnisse beim überwachten Objekt.

Nach **§ 6b BDSG** ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur dann zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher (Bundes-)Stellen,
2. zur Wahrnehmung des Hausrechtes oder
3. zur Wahrnehmung berechtigter Interessen für konkrete festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der beobachteten Betroffenen überwiegen.

Im Rahmen der Anhörung zur Bewertung einer festgestellten Videoüberwachung des öffentlich zugänglichen Raumes holt der Landesbeauftragte von dem Betreiber (verantwortlichen Stelle) zunächst Informationen darüber ein, welche Interessen mit der Videoüberwachung verfolgt werden. Dabei genügt die Mitteilung in der Regel nicht, einer abstrakten Gefahrenlage zum Schutz des Eigentums begegnen zu wollen (z. B. Versuch der Verhinderung von Graffiti und Schmierereien). Vielmehr müssten belegbare Angaben die Annahme rechtfertigen, dass weitere Beeinträchtigungen der Rechte der verantwortlichen Stelle drohen.

Bei Gebäuden, deren Fassade direkt an den öffentlichen Gehweg grenzt, ist jedoch eine Videoüberwachung der Fassade ohne gleichzeitige Mitüberwachung von Teilen des Gehweges unmöglich. Eine unvermeidbare Mitüberwachung von maximal einem Meter des öffentlichen Gehweges bzw. der Straße erscheint in solchen Fällen noch hinnehmbar. Jedoch müssen im Einzelfall die Persönlichkeitsrechte der Passanten gegen die berechtigten Interessen des Gebäudeeigentümers, z. B. an einer wirksamen Graffiti-Abwehr, gegeneinander abgewogen werden. Das Amtsgericht Berlin (Urteil vom 18. Dezember 2003, Az.: 16 C 427/02, NJW-RR 2004, 531) hatte den für die Videoüberwachung einer Hausfassade Verantwortlichen dazu verurteilt, „*die Videoüberwachung mittels der Videokamera ... zu unterlassen, soweit diese über einen 1 Meter breiten Streifen entlang der Schaufensterseite … hinausgeht*“.

Außerdem ist zu beachten, dass die Mitüberwachung eines Hauseinganges durchaus einen erheblichen Eingriff in das Persönlichkeitsrecht und das Selbstbestimmungsrecht eines Mieters und seines Besitzrechtes an der gemieteten Wohnung darstellen kann. Sie kann allenfalls dann gerechtfertigt sein, wenn ein berechtigtes Überwachungsinteresse der Gemeinschaft das Interesse des einzelnen Wohnungseigentümers und von Dritten, deren Verhalten mitüberwacht wird, überwiegt und wenn die Ausgestaltung der Überwachung unter Berücksichtigung von § 6b BDSG inhaltlich und formell dem Schutzbedürfnis des Einzelnen ausreichend Rechnung trägt (vgl. Urteil des Bundesgerichtshofs vom 24. Mai 2013, Az.: V ZR 220/12, ZD 2013, 447).

Video(mit)überwachung nachbarschaftlicher Grundstücke

In einer ganzen Reihe von Fällen hatten die beim Landesbeauftragten vorgetragenen Beschwerden Videoüberwachungen nachbarschaftlicher Grundstücke zum Inhalt. Diese Art der Erhebung und Verarbeitung personenbezogener Daten erfolgt zumeist für persönliche oder familiäre Tätigkeiten. Damit bleiben sie nach § 1 Abs. 2 Nr. 3 BDSG dem Geltungsbereich des BDSG verschlossen. Wegen Nichtanwendbarkeit des BDSG ist dem Landesbeauftragten das Eingreifen in diesen Fällen versagt.

Jedoch wird den Betroffenen einer nachbarschaftlichen Kameraüberwachung in der Regel durch den Landesbeauftragten mitgeteilt, dass sie

rechtlich nicht schutzlos sind. Für sie könnte im Einzelfall ein aus §§ 823, 1004 BGB i. V. m. Art. 2 Abs. 1 GG folgender Anspruch auf Unterlassung der Videoüberwachung gegen den Kamerabetreiber in Betracht kommen. Die Überwachung der Grundstücke und Häuser Dritter durch eine Kamera kann – unabhängig davon, ob eine Speicherung von Aufnahmen oder auch eine Tonüberwachung erfolgt – einen erheblichen Eingriff in das Persönlichkeitsrecht und das Selbstbestimmungsrecht des Eigentümers und sein Besitzrecht an dem Grundstück darstellen (vgl. Urteil des Amtsgerichtes München vom 16. Oktober 2009, Az.: 423 C 34037/08). Es entsteht ein „Überwachungsdruck“, und zwar unabhängig davon, ob eine Videoaufzeichnung im Einzelfall tatsächlich erfolgt. Durch die Kamera kann sich der Bewohner in seinem privaten Bereich nicht mehr ungestört und unbeobachtet fühlen. Das allgemeine Persönlichkeitsrecht umfasst auch die Freiheit von ungewünschter Kontrolle oder Überwachung durch Dritte (vgl. Urteil des Amtsgerichtes Schöneberg vom 8. Juni 2012 – Az.: 19 C 166/12).

Vermeintliche Video(mit)überwachung nachbarschaftlicher Grundstücke

In der aufsichtsbehördlichen Praxis sind dem Landesbeauftragten auch Fälle bekannt geworden, in denen neben der legitimen Videoüberwachung des eigenen Grundstückes auch eine Videomitüberwachung des nachbarschaftlichen Grundstückes zwar nicht offensichtlich vorlag, der betroffene Bewohner jedoch glaubte, einer solchen Videoüberwachung ausgesetzt zu sein. Mangels Erhebung personenbezogener Daten liegt kein datenschutzrelevanter Vorgang vor. Auch in einem solchen Fall ist wegen der Nichtanwendbarkeit des BDSG eine Kontrollkompetenz des Landesbeauftragten nicht gegeben. Er kann deshalb nicht aufsichtsbehördlich tätig werden. Jedoch kann durch die Installation von Überwachungskameras auf einem privaten Grundstück das Persönlichkeitsrecht des vermeintlich überwachten Nachbarn schon aufgrund einer Verdachtssituation durch den entstehenden Überwachungsdruck beeinträchtigt sein. Allein die hypothetische Möglichkeit einer Überwachung reicht dazu aber nicht aus (siehe dazu Urteil des Bundesgerichtshofes vom 16. März 2010, Az. VI ZR 176/09, NJW 2010, 1533). Es komme bei der Beurteilung, ob ein Beseitigungsanspruch bestehen könnte, insoweit auf die Umstände des Einzelfalles an. In Bezug auf einen möglicherweise bestehenden Beseitigungsanspruch wird auf den Beitrag zu Kameraattrappen (Nr. 4.17.8) verwiesen. Nach der Rechtsprechung des Oberlandesgerichts München besteht ein Abwehranspruch gegen die Installation einer privaten Videoüberwachungsanlage nur dann, wenn der Betroffene eine Überwachung durch die Überwachungskamera objektiv ernsthaft befürchten muss (Urteil des Oberlandesgerichtes München vom 13. Februar 2012, Az. 20 U 4641/11, CR 2012, 335).

Aufzeichnung

Das Aufzeichnen ist datenschutzrechtlich ein Speichern und damit ein Verarbeitungsprozess (§ 3 Abs. 4 Nr. 1 BDSG). Dieser bedarf der gesonderten Prüfung anhand der Zulässigkeitsvoraussetzungen des § 6b Abs. 3 Satz 1 BDSG. Auch die Tatsache der über die Beobachtung hinausge-

henden Speicherung bedarf daher der gesonderten Abwägung mit den berechtigten Interessen der Betroffenen. Nach § 6b Abs. 5 BDSG sind die aufgezeichneten (gespeicherten) Daten dann unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks (§ 6b Abs. 1 BDSG) nicht mehr erforderlich sind. Sie sind nach § 6b Abs. 5 BDSG im Übrigen auch dann zu löschen, wenn zwar der beabsichtigte Zweck der Speicherung noch nicht erreicht ist, jedoch schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Erkennbarmachung einer Videoüberwachung

Die Tatsache, dass ein öffentlich zugänglicher Raum videoüberwacht wird, ist nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen ebenso erkennbar zu machen wie die Identität der verantwortlichen Stelle. Eine geeignete Maßnahme wäre z. B. ein ausreichend großes Hinweisschild oder ein Aufkleber an präsenter Stelle. Einen solchen Hinweis sollte der Betroffene beim Betreten des überwachten Bereiches im Blick haben können, ohne ihn suchen zu müssen. Unter Umständen ist mehr als ein Hinweisschild anzubringen.

4.17.3 Videoüberwachung im Unternehmen

Überwachung des Publikumsbereiches

Beim Publikumsbereich in einem Unternehmen, z. B. dem Kundenempfang oder schlicht dem Verkaufsraum, wird es sich meist um einen öffentlich zugänglichen Raum handeln. Unter öffentlich zugänglichen Räumen sind nicht nur umbaute, sondern auch nicht umbaute Flächen zu verstehen, die nach dem erkennbaren Willen des Berechtigten den Zweck haben oder dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Demnach beurteilt sich die Zulässigkeit der Beobachtung mit optisch-elektronischen Einrichtungen und damit die Erhebung personenbezogener Daten in diesen Fällen nach § 6b Abs. 1 Nrn. 2 und 3 BDSG.

Das Hausrecht (§ 6b Abs. 1 Nr. 2 BDSG) beinhaltet die Befugnis darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objektes und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann zum einen präventive Zwecke verfolgen, aber auch als repressives Mittel zur Beweissicherung eingesetzt werden. In Betracht kommen derartige Maßnahmen z. B. in unübersichtlichen Verkaufsräumen. Verhindert oder aufgedeckt werden, sollen in der Regel Ladendiebstähle. Jedoch ist auch in diesen Fällen eine Abwägung der Interessen des Betreibers an möglichst geringen Inventurdifferenzen mit den schutzwürdigen Interessen der Kundschaft am nichtüberwachten Einkaufserlebnis erforderlich.

Der Landesbeauftragte weist jedoch auf einen weiteren Aspekt bei der Videoüberwachung des Kundenbereiches eines Unternehmens hin: Der Kundenbereich ist häufig auch Arbeitsbereich von Beschäftigten. Insoweit besteht eine erheblich andere Interessenlage als bei nur vorübergehend anwesenden Kunden. Dennoch können Sicherheitsbedürfnisse die Beobachtung legitimieren, wie z. B. in den Verkaufsräumen eines Kaufhauses. Dann müssen Mitarbeiter die Beobachtung als arbeitsplatzimmanent hinnehmen. Zweck einer Videoüberwachung im Kundenbereich eines Einkaufsmarktes wird regelmäßig die Kundenbeobachtung zur Senkung der Diebstahlquote sein. Eine Auswertung der Kamerabilder zur Mitarbeiterüberwachung wäre somit unzulässig.

Liegt eine Videoüberwachung eines öffentlich zugänglichen Raumes vor, ist nach § 6b Abs. 2 BDSG der Umstand der Beobachtung und die dafür verantwortliche Stelle, soweit diese nicht offensichtlich ist, erkennbar zu machen. Das gilt auch für Kundenbereiche von Einkaufsmärkten oder Banken.

Überwachung der Mitarbeiter, die nicht in öffentlich zugänglichen Bereichen beschäftigt sind

In der Regel handelt es sich bei der Videoüberwachung von Arbeitnehmern um eine Erhebung und ggf. Verarbeitung personenbezogener Daten im Rahmen des Beschäftigungsverhältnisses – natürlich nur, soweit der Beschäftigte auf den Aufnahmen erkenn- oder identifizierbar ist. § 32 Abs. 1 BDSG gestattet, dass personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben und verarbeitet werden dürfen, soweit dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn dokumentierte tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und dass schutzwürdige Interessen des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegen. Art und Ausmaß der Überwachung dürfen dabei im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Für die Rechtmäßigkeit einer Videoüberwachung im Arbeitsverhältnis ist eine Güterabwägung erforderlich, die die Umstände des Einzelfalls berücksichtigt. Der Verhältnismäßigkeitsgrundsatz ist zu beachten. Maßgeblich sind daher die Eingriffsintensität und damit der psychische Anpassungsdruck; die Einschränkung der Freiheit, selbstbestimmt zu handeln; die Unsicherheit, ob Verhaltensweisen notiert, gespeichert, weitergegeben oder ignoriert werden, sowie die überwiegende Betroffenheit Unschuldiger, also von Personen, gegen die kein Verdacht besteht. Bei öffentlich zugänglichen Räumen (§ 6b BDSG) ist der überwachte Personenkreis zunächst unbekannt. Innerhalb eines Beschäftigungsverhältnisses sind die Personen sehr wohl bekannt und die Beobachtung findet unter Umständen über einen längeren Zeitraum statt. Der Beschäftigte verbleibt auch

nicht freiwillig am Arbeitsplatz, vielmehr erfolgt die Zuweisung im Rahmen des Direktionsrechts durch den Vorgesetzten.

Eine heimliche Videoüberwachung eines Arbeitnehmers kann zulässig sein, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachtes ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit praktisch das einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist (vgl. Urteil des Bundesarbeitsgerichtes vom 21. Juni 2012, NJW 2012, 3594). Der Verdacht muss in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlungen zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern bestehen.

Dem Landesbeauftragten sind aber auch Fälle bekannt geworden, in denen präventiv zum Zweck der Verhinderung von Mitarbeiterdiebstählen eine offene Videoüberwachungsanlage installiert worden ist. Um es sich möglichst leicht zu machen, hatte die Unternehmensführung dafür die Einwilligung ihrer nun unter Dauerüberwachung stehenden Beschäftigten eingeholt. Jedoch wird in der Regel aufgrund des Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber eine wichtige Einwilligungsvoraussetzung fehlen: Die vom Arbeitgeber im Streitfall nachzuweisende Freiwilligkeit!

In einem vom Landesbeauftragten kontrollierten Fall hatte ein Arbeitgeber seine Autowerkstatt wegen durch Mitarbeiter begangener Materialdiebstähle und Abrechnungsbetrügereien komplett videoüberwacht. Dabei wäre im konkreten Fall nur die Anzahl der in die Werkstatt fahrenden Autos von Bedeutung gewesen. Der Landesbeauftragte konnte in diesem Fall erreichen, dass alternativ zur Totalüberwachung ausschließlich die Werkstattzufahrt von oben herab inklusive eines schmalen Bereichs des Werkstattraumes überwacht wurde. Dadurch wurden die erbrachten Dienstleistungen zählbar, ohne die Beschäftigten einer ständigen Videoüberwachung auszusetzen.

4.17.4 Videoüberwachung in Restaurants

Aus verfassungsrechtlichen Gründen, nämlich als Ausfluss des Rechts auf informationelle Selbstbestimmung, sollen die Bürgerinnen und Bürger das Recht haben, ihre Freizeit, zu der auch Restaurantbesuche zählen, unbeobachtet zu genießen.

Für jedermann zugängliche Gastwirtschaften bzw. Restaurants fallen ebenfalls grundsätzlich unter die in § 6b BDSG genannten öffentlichen Räume, in denen eine Beobachtung mit optisch-elektronischen Geräten erst nach einer umfassenden Güter- und Interessenabwägung unter Beachtung der rechtlich geschützten Positionen sämtlicher Beteiligter und unter Würdigung der Umstände zulässig werden könnte. Es dürfen keine Anhaltspunkte dafür sprechen, dass schutzwürdige Interessen der betroffenen Gäste überwiegen. Hierbei ist zu berücksichtigen, dass die Gäste

das Restaurant als Rückzugsraum aufsuchen. Durch Sitzbereiche an Tischen wird zu längerem Aufenthalt eingeladen. Gäste sollen ungestört und entspannt einen längeren Aufenthalt genießen können. Außerdem ist zu berücksichtigen, dass ggf. durch Beobachtungen des Gastraumes auch Mitarbeiter erfasst werden können. Hinsichtlich der Mitarbeiterüberwachung ist ein besonders strenger Maßstab anzulegen. Nach der Rechtsprechung kann eine Videoüberwachung der Mitarbeiter allenfalls dann in Betracht kommen, wenn eine notwehrähnliche Lage gegeben ist (vgl. Nr. 4.17.3).

Eine Videoüberwachung von Kunden und Mitarbeitern in Gastwirtschaften bzw. Restaurants ist daher i. d. R. unzulässig.

4.17.5 Videoüberwachung mit Außen- und Innenkameras bei Taxis

Der Landesbeauftragte hatte sich im Berichtszeitraum mit beiden Komplexen beschäftigt. Zu beantworten waren Fragen in Bezug auf die Überwachung des Straßenraumes vor dem fahrenden Taxi ebenso wie Fragen in Bezug auf die Videoüberwachung des Taxi-Innenraumes – also der Fahrgäste.

Videoüberwachung des Straßenraumes vor dem Taxi

Die Videoüberwachung des Straßenraumes vor einem fahrenden Taxi geht auf ein Projekt einer deutschen Versicherung zurück. Die Verwendung einer „Taxenunfallkamera“ sollte als eine Zusatzoption zur Kfz-Versicherung konzipiert werden. Ziel sei gewesen, kritische Verkehrssituationen und Unfälle nachvollziehen und auswerten zu können. Auf diese Weise solle die Verkehrssicherheit im Bereich der gewerblichen Personenbeförderung erhöht und indirekt auf das Fahrverhalten der Taxifahrer Einfluss genommen werden. Technisch war beabsichtigt, am Innenspiegel eine mit einem Beobachtungswinkel von 170 Grad nach vorn blickende Kamera zu installieren. Zugriff auf die nach 72 Aufnahmestunden automatisch gelöschten Bilddateien habe nur der Taxiunternehmer – das muss nicht der Fahrer sein – und im Fall eines Unfalls möglicherweise das Versicherungsunternehmen. Dies könnte einerseits bei risikoreicher Fahrweise dazu führen, dass die Versicherungsprämie erhöht würde. Andererseits könnte sich der Taxifahrer einen Beweisvorteil bei unberechtigten Schadenersatzforderungen Dritter verschaffen.

Der Düsseldorfer Kreis, ein bundesweites Gremium der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, hat hierzu folgenden Beschluss gefasst:

„Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher beweissichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und evtl. nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Auf-

schriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern oder Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird."

Die Ausstattung von Taxis mit Unfallkameras, wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig (vgl. den Beschluss des Düsseldorfer Kreises vom 26. und 27. Februar 2013 „Videoüberwachung in und an Taxis").

Videoüberwachung des Taxi-Innenraumes

Datenschutzrechtlich stellt sich der Taxi-Innenraum als öffentlich zugänglicher Raum dar. Dessen Beobachtung mit optisch-elektronischen Einrichtungen unterliegt ebenfalls § 6b BDSG. Die Innenraumüberwachung kann sowohl der Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) als auch der Abwehr von Gefahren für Leben und Gesundheit der Fahrer (§ 6b Abs. 1 Nr. 3 BDSG) dienen. Sie muss verhältnismäßig und vor allem erforderlich sein (§ 6 Abs. 3 BDSG). Das könnte z. B. dann zutreffen, wenn sich zuvor konkrete Vorkommnisse in Form von Übergriffen auf die Fahrer des Unternehmens ereigneten und wenn nach allgemeiner Lebenserfahrung tatsächlich mit weiteren Übergriffen gerechnet werden muss. Für eine besonders kritische Würdigung spricht, dass die Fahrgäste des Taxis nicht in überwachungsfreie Räume ausweichen können. Vor dem Hintergrund sieht der Landesbeauftragte die Videoüberwachung des Taxi-Innenraumes nur in außerordentlich engen Grenzen als rechtlich zulässig an.

In dem o. g. Beschluss des Düsseldorfer Kreises (**Anlage 32**) werden die Rahmenbedingungen für eine Innenraumüberwachung klar dargestellt:

„Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines ‚stillen Alarms' oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich perma-

nent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist."

Im Dezember 2011 ist dem Landesbeauftragten durch die Medien bekannt geworden, dass eine große Taxigenossenschaft in seinem Zuständigkeitsbereich die Ausstattung ihrer Wagen mit Innenraumkameras plant. Das durch ihn unterbreitete Beratungsangebot wurde spät angenommen, führte aber dazu, dass die o. a. Maßstäbe stärkere Beachtung erfuhren.

4.17.6 Wildkameras

Grundsätzlich wird sich ein Jäger dafür interessieren, welches Wild sich in seinem Revier aufhält. Die moderne Technik bietet – in Form von gut getarnten Wildkameras – eine einfache Möglichkeit, das zu ermitteln. Wildkameras, im Fachhandel ab ca. 100 Euro erhältlich, sind mit Bewegungs- oder Infrarotsensor ausgestattet. Sie verfügen i. d. R. über einen unsichtbaren Infrarotblitz und eine gute Bildauflösung. Die Aufnahmen mit Datum gespeichert oder bei Premium-Geräten zum Handy oder per E-Mail gesendet. Solch ein Gerät liefert scharfe Bilder von allem, was in den Aufnahmebereich gerät. Personen, von denen Wildkameras Aufnahmen fertigen würden, dürfen grundsätzlich nach § 3 Abs. 1 Feld- und Forstordnungsgesetz (FFOG) den Wald, auch außerhalb der Wege, betreten. Damit wird deutlich, dass es sich beim Wald ebenfalls um öffentlich zugänglichen Raum handelt. Dessen Beobachtung mit optisch-elektronischen Einrichtungen ist nur im Rahmen des § 6b BDSG zulässig.

Nach § 6b Abs. 1 Nr. 3 BDSG könnte eine Überwachung mittels Wildkamera zulässig sein, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Solche Zwecke könnten z. B. besondere Anforderungen an die Hege oder besonders intensive Wildbeobachtungen im Rahmen tierschutzgerechten Weidwerkes sein.

Jedenfalls ist im Einzelfall zu prüfen, ob diese berechtigten Interessen der verantwortlichen Stelle, also des Jagdausübungsberechtigten, die unter Umständen schutzwürdigen Interessen der betroffenen Waldbesucher wirklich überwiegen.

Die Wildkamera sollte so aufgestellt werden, dass sie entweder nur bodennahe Aufnahmen macht oder Aufnahmen von oben herab, um die Gefahr der Identitätsaufdeckung der versehentlich abgebildeten Personen zu minimieren. Keinesfalls sollte eine Wildkamera einen Weg (mit)-überwachen.

Nach § 6b Abs. 5 BDSG sind die personenbezogenen Daten, also die Aufnahmen der Wildkamera von Personen, unverzüglich zu löschen, wenn sie nicht mehr erforderlich sind. Im Fall der Wildkamera bedeutet das „sofort“, also ohne schuldhaftes Zögern, da eine Erforderlichkeit überhaupt nicht gegeben ist.

Auch für Wildkameras gilt im Übrigen eine Kennzeichnungspflicht nach § 6b Abs. 2 BDSG. Der Umstand der Beobachtung und die verantwortliche Stelle sind erkennbar zu machen (siehe hierzu Nr. 4.17.2). Das BDSG lässt keinen Raum, von dieser Verpflichtung abzusehen, auch wenn durch die Kennzeichnung der Diebstahl der Kamera wahrscheinlicher sein könnte.

Datenschutzrechtlich anders zu bewerten ist die Ausstellung einer Wildkamera in einem Naturschutzgebiet, über die sich ein Petent beim Landesbeauftragten beschwerte. Nach der Verordnung, auf deren Grundlage das Naturschutzgebiet eingerichtet worden war, war es verboten, sich dort außerhalb von Wegen aufzuhalten. Damit wird deutlich, dass der von dieser Kamera beobachtete Wald kein öffentlich zugänglicher Raum war, auch wenn die ordnungsgemäße Jagd im Naturschutzgebiet zulässig war. Damit ist § 6b BDSG nicht anwendbar.

4.17.7 Webcams

Schon seit vielen Jahren ist der Trend zu beobachten, dass von Gewerbetreibenden speziell aus dem Hotel- und Gaststättenbereich, aber auch von Baubetrieben und selbst von Privatpersonen zu den unterschiedlichsten Zwecken Livebilder von interessanten Orten ins Internet gestellt werden, wo sie von jedermann betrachtet werden können.

Seitdem im November 1993 die erste Webcam der Welt ihre in 142x159 Punkte aufgelösten Graustufenbilder ins Internet sandte – gezeigt wurde der Füllstand einer Kaffeemaschine im Rechnerlabor der University of Cambridge – sind nicht nur viele Jahre vergangen, sondern auch die technischen Möglichkeiten aktueller Webcams haben sich wesentlich verbessert. Selbst preisgünstige Webcams liefern Standbilder und Videos in HD-Auflösung. Damit könnten in einer abgebildeten Szenerie Menschen durchaus erkennbar werden, wodurch der Einsatz von diesen Webcams datenschutzrechtlich relevant wird.

Sind Personen identifizierbar, ist der Betrieb der Webcam nur unter den in § 6b Abs. 1 BDSG genannten Einschränkungen und bei Beachtung des Rechtes der Abgebildeten nach §§ 22, 23 des KunstUrhG zulässig. Nach § 23 Abs. 1 Nr. 2 KunstUrhG müsste die Überprüfung im Einzelfall ergeben, dass die abgebildete Person nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheint.

Die weltweite Veröffentlichung von Foto- oder Videoaufnahmen mit erkennbaren Personen über das Internet an die Allgemeinheit ist eine Übermittlung personenbezogener Daten. Nach § 3 Abs. 4 Nr. 3 BDSG stellt auch die Übermittlung personenbezogener Daten eine relevante Phase einer Datenverarbeitung dar. Jedoch ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 4 Abs. 1 BDSG nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine gesetzliche Grundlage für eine Übermittlung mittels Webcam gewonnener personenbezogener Daten in das Internet ist, mit den dort genannten Einschränkungen, im o. g. § 23 Abs. 1 Nr. 2 KunstUrhG zu finden. Von vornherein ausscheiden dürfte dagegen eine Einwilligungslösung aufgrund des unbestimmten und auch faktisch nicht bestimmbaren Betroffenenkreises. Nicht als Einwilligung durch konkludentes Handeln kann das Betreten des beobachteten Bereiches in vorheriger Kenntnis der Tatsache der Beobachtung gewertet werden.

Der Landesbeauftragte empfiehlt jedoch zur Vermeidung von Irritationen und Streitigkeiten die Blickrichtung und Bildauflösung der Kamera so zu wählen, dass Menschen auch mit Zusatzkenntnis nicht identifizierbar sind.

4.17.8 Kameraattrappen

Für einen Betroffenen oft nicht zu unterscheiden ist eine echte Überwachungskamera von einer täuschend echt aussehenden Attrappe. Tatsächlich kann von einer solchen Attrappe eine gleichwertige Persönlichkeitsrechtsbeeinträchtigung des Betroffenen ausgehen wie von einer echten Kamera. Es entsteht eine Art Überwachungsdruck (vgl. Urteil des Bundesgerichtshofs vom 16. März 2010, NJW 2010, 1533).

In einer Vielzahl von Fällen musste der Landesbeauftragte beschwerdeführenden Betroffenen mitteilen, dass das BDSG nicht anwendbar ist, weil mit einer Attrappe keine personenbezogenen Daten erhoben werden. Dem Landesbeauftragten bleibt lediglich die Kontrolle bei der verantwortlichen Stelle, ob es sich tatsächlich um eine Attrappe handelt (siehe Nr. 4.17.2).

Es ist möglich, dass der Betroffene gegenüber dem „Betreiber“ einer Kameraattrappe einen zivilrechtlichen Beseitigungsanspruch haben kann, wobei es, so der Bundesgerichtshof (a. a. O.), auf die Umstände des Einzelfalls ankomme.

4.18 Prangerwirkung des Internets

Zeitungsarchiv im Internet

Ein Petent beklagte, dass in einem Internetarchiv einer Lokalzeitung Texte recherchierbar seien, die auf seine frühere strafgerichtliche Verurteilung hinwiesen. Dies wirke weiter beeinträchtigend, obwohl die Verurteilung nicht mehr im Bundeszentralregister geführt werde.

Der Landesbeauftragte vermochte jedoch nicht zu helfen, da § 38 BDSG, der die Befugnisse als Aufsichtsbehörde im nicht öffentlichen Bereich regelt, gemäß § 41 Abs. 1 BDSG nicht für Presseveröffentlichungen zu journalistisch-redaktionellen Zwecken gilt. Dies wird als sog. Medienprivileg bezeichnet, das in Sachsen-Anhalt durch § 10a PresseG umgesetzt ist. Es betrifft auch Presseartikel, die über das Internet abrufbar sind.

Der Landesbeauftragte konnte ergänzend darauf hinweisen, dass das Bereithalten der den Betroffenen Angeklagten bzw. Verurteilten bezeichnende Meldungen zum Abruf im Internet grundsätzlich einen Eingriff in das allgemeine Persönlichkeitsrecht darstellt. Dies gilt auch bei einer passiven Darstellungsplattform. Zivilrechtliche Ansprüche bleiben möglich. Nach der Rechtsprechung des Bundesgerichtshofs verdient das Informationsinteresse der Öffentlichkeit bei der Abwägung mit der damit zwangsläufig verbundenen Beeinträchtigung des Persönlichkeitsrechts des Täters im Rahmen aktueller Berichterstattung über schwerwiegende Straftaten im Allgemeinen den Vorrang (vgl. Urteil vom 9. Februar 2010, NJW 2010, 2432). Das Persönlichkeitsrecht und das Wiedereingliederungsinteresse schützen zwar vor unbegrenzter öffentlicher Diskussion. Je nach Intensität der Beeinträchtigung des Persönlichkeitsrechts hat der Schutz der Persönlichkeit und die Achtung des Privatlebens hinter dem verfolgten Informationsinteresse der Öffentlichkeit und dem Recht auf freie Meinungsäußerung zurückzutreten. Bei Tatsachenberichten hängt die Abwägung zwischen den widerstreitenden Interessen u. a. vom Wahrheitsgehalt ab. Wahre Aussagen müssen in der Regel hingenommen werden, auch wenn sie nachteilig für den Betroffenen sind (vgl. BVerfG, Beschluss vom 25. Januar 2012, NJW 2012, 1500).

Bewertungsportale

Im IX. Tätigkeitsbericht (Nr. 20.6) wurde die Problematik der Bewertungsportale bereits angesprochen. Im Vordergrund stand die Rechtsprechung des Bundesgerichtshofs zu einem Lehrerbewertungsportal. Der darin formulierte weitreichende Schutz der Meinungsäußerungsfreiheit wurde zwischenzeitlich durch obergerichtliche Rechtsprechung auch anderen Portalen zugebilligt. Das Oberlandesgericht Frankfurt (NJW 2012, 2898) hat in Bezug auf ein Arztbewertungsportal auch anonyme Bewertungen akzeptiert. Wäre eine Verpflichtung gegeben, sich zu einer Meinung zu bekennen, bestünde die Gefahr einer grundrechtseinschränkenden Selbstzensur. Gegen Missbrauch wirkte u. a. die Angabe der E-Mail-Adresse. Weiter wurde akzeptiert, dass das konkrete Portal über Suchmaschinen recherchierbar war. Vor dem Hintergrund freier Arztwahl und dem Wett-

bewerb seien Ärzte den Marktmechanismen ausgesetzt. Dazu gehört auch, dass die Meinungsfreiheit die Wahl des Verbreitungsmediums gewährleistet. Im Zusammenhang mit einigen Sicherungsmaßnahmen war die Äußerung in einem Portal nach umfassender Abwägung daher zulässig. Gewisse Sicherungen sind geboten, um dem Schutz der Persönlichkeitsrechte der Bewerteten Rechnung zu tragen.

Die Datenschutzaufsichtsbehörden, in deren Zuständigkeitsbereich Arztbewertungsportale tätig sind, haben sich mit der Thematik befasst und eine Orientierungshilfe erarbeitet. Die „Leitlinie mit Mindestanforderungen für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet“ vom 14. März 2013 kann beim Landesbeauftragten angefordert werden.

4.19 Soziale Netzwerke

4.19.1 Nutzung sozialer Netzwerke durch öffentliche Stellen

Obwohl nachvollziehbar ist, dass öffentliche Stellen mit ihren Informationen und Angeboten auch jüngere Internetnutzer erreichen möchten, die zu einem großen Prozentsatz in sozialen Netzwerken aktiv sind, bestehen bezüglich der Einrichtung von Fanpages auf Facebook erhebliche datenschutzrechtliche Bedenken.

Grundlage und Maßstab für das Handeln öffentlicher Stellen des Landes ist das Rechtsstaatsprinzip. Die öffentlichen Stellen sind an Recht und Gesetz gebunden (Art. 20 Abs. 3 GG). Sie sind dafür verantwortlich, dass sie rechtmäßig handeln, vor allem dann, wenn es um die Erhebung und Verarbeitung personenbezogener Daten geht. Aus diesem Grund sollte die Nutzung sozialer Netzwerke wie Facebook, die nicht mit deutschem bzw. europäischem Datenschutzrecht in Einklang stehen, vermieden werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben Facebook wiederholt in Schreiben, bei Besprechungen und im Rahmen von Veröffentlichungen auf die datenschutzrechtlichen Anforderungen an soziale Netzwerke hingewiesen (**Anlagen 25, 29**). Die derzeitige Ausgestaltung von Facebook widerspricht jedoch in vielen Punkten diesen Anforderungen. Zahlreiche Funktionen verstoßen gegen deutsches Datenschutzrecht.

Dazu zählen nicht nur die Reichweitenanalyse durch den Like-it-Button, sondern auch die Gesichtserkennungsfunktion und der Freundefinder. Das Landgericht Berlin hat in seinem Urteil vom 6. März 2012 (Az.: 16 O 551/10) festgestellt, dass Facebook mit dem Freundefinder und seinen Geschäftsbedingungen gegen Verbraucherrechte verstößt. Das Gericht urteilte, die Nutzer müssten klar und deutlich informiert werden, dass durch den Freundefinder ihr gesamtes Adressbuch zu Facebook übertragen und für Freundeseinladungen genutzt wird. Dies fand bislang nicht statt. Weiterhin urteilte das Gericht, Facebook dürfe sich in seinen Allgemeinen Geschäftsbedingungen nicht ein umfassendes weltweites und

kostenloses Nutzungsrecht an Inhalten einräumen lassen, die Facebook-Mitglieder in ihr Profil einstellen. Rechtswidrig ist nach Auffassung der Richter ferner die Einwilligungserklärung, mit der die Nutzer der Datenverarbeitung zu Werbezwecken zustimmen. Zudem muss Facebook sicherstellen, dass es über Änderungen der Nutzungsbedingungen und Datenschutzbestimmungen rechtzeitig informiert. Gegen das Urteil hat Facebook Berufung eingelegt.

Des Weiteren verlangt Facebook von seinen Nutzern, sich mit ihrem realen Namen zu registrieren. Da diese Klarnamenpflicht gegen § 13 Abs. 6 TMG verstößt, hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) bereits Anordnungen nach § 38 Abs. 5 BDSG gegen Facebook erlassen. Allerdings stellte das Schleswig-Holsteinische Verwaltungsgericht in seinen Beschlüssen vom 14. Februar 2013 fest, dass das ULD seine Anordnung zu Unrecht auf das deutsche Datenschutzrecht gestützt habe, da die irische Niederlassung von Facebook für die Nutzerdatenverarbeitung in Europa zuständig ist und demzufolge irisches Datenschutzrecht Anwendung findet. Diese Auffassung teilt auch das Oberverwaltungsgericht Schleswig und hat am 22. April 2013 die Beschwerden des ULD gegen die Beschlüsse des Verwaltungsgerichts zurückgewiesen (Az.: 4 MB 10/13, 4 MB 11/13).

Weitere Funktionen wie z. B. die neue Suchfunktion Graph Search und Facebook Home ermöglichen es Facebook, immer weiter in die Privatsphäre seiner Nutzer einzudringen, aber auch in die Persönlichkeitsrechte Dritter, die nicht Mitglieder bei Facebook sind, einzugreifen.

Die Formulierungen in den Nutzungsbedingungen und Datenschutzrichtlinien von Facebook genügen nicht den Anforderungen an eine wirksame und informierte Einwilligung gem. § 4a Abs. 1 BDSG bzw. § 4 Abs. 2 DSG LSA. So legt Facebook z. B. einfach fest, dass der Nutzer durch den Zugriff auf und die Nutzung von Facebook den Nutzungsbedingungen zustimmt. Dabei geht Facebook davon aus, dass der Nutzer auch zukünftigen Aktualisierungen zustimmt, die ihm mit einer Frist von 7(!) Tagen bekannt gegeben werden. Laut Facebook erteilt der Nutzer seine Einwilligung, indem er auf „Registrieren“ klickt. Damit würde er die Nutzungsbedingungen akzeptieren und erklären, die Datenverwendungsrichtlinien sowie die Bestimmungen zur Verwendung von Cookies gelesen zu haben.

Facebook vertritt den Standpunkt, dass für die automatisierte Verarbeitung der Nutzerdaten nicht deutsches, sondern irisches Datenschutzrecht gilt und damit auch die Zuständigkeit der deutschen Datenschutzaufsichtsbehörden nicht gegeben ist. Selbst wenn man wie das Oberverwaltungsgericht Schleswig-Holstein dieser Aussage folgt, gelten für öffentliche Stellen in Sachsen-Anhalt das Landesdatenschutzgesetz sowie bereichsspezifische Datenschutzregelungen. Öffentliche Stellen, die Informationsangebote im Internet veröffentlichen, müssen die Regelungen des TMG beachten. Mit der Einrichtung einer Fanpage bei Facebook können sie diesen Verpflichtungen jedoch nicht nachkommen.

Der Bayerische Landesbeauftragte für den Datenschutz hat am 28. März 2013 eine Orientierungshilfe „Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit“ herausgegeben. Darin wird anhand der Vorschriften des TMG erläutert, aus welchen Gründen die Einrichtung und Nutzung einer Fanpage auf Facebook derzeit nicht datenschutzkonform möglich ist.

Datenschutzrechtlich besonders kritisch ist die Kommentierungsfunktion. Wird dem Nutzer einer Fanpage die Möglichkeit zur Kommunikation eingeräumt und nutzt er diese, erhält Facebook durch die Kommentare weitere Nutzerdaten. Werden die Nutzer zur öffentlichen Äußerung politischer Meinungen ermuntert, handelt es sich dabei um personenbezogene Daten besonderer Art (§ 2 Abs. 1 Satz 2 DSG LSA), die einem besonderen Schutz unterliegen.

Bereits im letzten Jahr hat die Innenministerkonferenz einen Bericht ihres Arbeitskreises I „Staatsrecht und Verwaltung“ zum Datenschutz in Sozialen Netzwerken zur Kenntnis genommen, der von der Konferenz der Chefs der Staats- und Senatskanzleien der Länder in Auftrag gegeben wurde und der unter anderem zu folgendem Ergebnis kommt: „Öffentliche Stellen trifft bei der Öffentlichkeitsarbeit mittels Sozialer Netzwerke die Pflicht, hierbei sorgfältig auf ein hohes Datenschutzniveau zu achten. […] Bei Fanpages sollte eine solche Mitverantwortung zumindest aufgrund einer ‚Vorbildfunktion‘ des Staates bejaht werden, der das Recht auf informationelle Selbstbestimmung seiner Bürgerinnen und Bürger schützen sollte.“ Zu diesen Fragestellungen und zum weiteren Vorgehen sind Innenministerkonferenz und Datenschutzkonferenz im Gespräch.

Fazit:

Der Landesbeauftragte empfiehlt – wie bereits die Datenschutzkonferenz (**Anlage 5**) – öffentlichen Stellen, auf die Einrichtung von Facebook-Fanpages zu verzichten. Dies galt schon vor den Enthüllungen über Ausspähungen durch den amerikanischen Geheimdienst, aber nun umso mehr. Verwiesen wird im Übrigen auf den Beitrag unter Nr. 5.6.

Schließlich besteht die Notwendigkeit eines verbindlichen Rechtsrahmens über die nationale Ebene hinaus, wie sich mit der europäischen Datenschutz-Grundverordnung abzeichnet (Nr. 3.1.1). Ein vom Bundesministerium des Innern im November 2011 angestoßener Selbstregulierungskodex der sozialen Netzwerke mit einer Orientierung an der deutschen Rechtslage scheiterte, weil sich unter anderem Facebook aus den Gesprächen mit der Freiwilligen Selbstkontrolle Multimedia zurückzog.

4.19.2 Nutzung sozialer Netzwerke für private oder familiäre Zwecke

Eine Petentin fragte an, ob die Aufnahme ihrer personenbezogenen Daten in einem sozialen Netzwerk durch einen Dritten zulässig sei. Der Eintrag sei auch für Freunde von Freunden sichtbar, allerdings nicht öffentlich.

Eine Prüfung durch den Landesbeauftragten für den Datenschutz als Aufsichtsbehörde nach § 38 BDSG kam jedoch nicht in Betracht. Der Anwendungsbereich des BDSG war nicht eröffnet. Nach § 1 Abs. 2 Nr. 3 BDSG ist zwar die Verarbeitung nicht-öffentlicher Stellen erfasst. Davon ausgenommen sind nach dieser Regelung aber das Erheben, Verarbeiten oder Nutzen von Daten ausschließlich für persönliche oder familiäre Tätigkeiten.

Mit der Regelung wird die persönliche Lebenssphäre von der beruflichen bzw. geschäftlichen Aktivität abgegrenzt. Unabhängig von der Datenmenge oder der Sensibilität der betroffenen Informationen entzieht sich der private Aktionskreis dem Regime des BDSG. Die eventuelle zivilrechtliche Verfolgung von Beeinträchtigungen des Persönlichkeitsrechts wird dadurch nicht eingeschränkt, lediglich datenschutzrechtlich ist eine Verfolgung ausgeschlossen.

Die Einordnung von Lebenssachverhalten in den privaten bzw. familiären Bereich richtet sich nach der Verkehrsanschauung. Typischerweise gehören hierzu u. a. die Bereiche Freizeit, Liebhabereien, Urlaub, privater Konsum oder Unterhaltung. Die Nutzung von Informationstechnologie (PC, Notebook, Smart-Phone usw.) zur Speicherung bzw. zum Transfer steht dem nicht entgegen.

Beim Austausch von Informationen innerhalb einer Organisation (z. B. Verein oder Fahrgemeinschaft) oder bei der Veröffentlichung von Daten auf einer allgemein zugänglichen Website im Internet wird der private Aktionskreis verlassen.

Bei Veröffentlichungen im Internet ist jedoch nicht zwingend der „öffentliche“ Bereich betroffen. Bei sog. postings ist, wie bei mündlichen Äußerungen, zwischen den Bereichen zu differenzieren. Die vertrauliche Kommunikation in der Privatsphäre ist Ausdruck des Persönlichkeitsrechts des Äußernden und grundrechtlich gewährleistet. Wie auch sonst, muss auch bei Internetäußerungen gelten, dass Äußerungen, die in der Öffentlichkeit einer kritischen Bewertung unterliegen, in Vertrauensbeziehungen als Ausdruck der Persönlichkeit und der Bedingungen ihrer Entfaltung Schutz genießen. Solange die Äußerung im privaten Kreis beabsichtigt ist und dieser Kreis nicht offensichtlich als öffentlich zu bewerten ist, kann sich der Äußernde auf die Vertraulichkeit stützen, auch wenn ggf. ein Empfänger die Information dann öffentlich macht. Auch ein sog. posting in privaten Bereichen öffentlicher Netzwerke kann daher grundsätzlich als dem privaten Bereich zugehörig zu verstehen sein. Ob der private Bereich durch Erreichen Dritter z. B. infolge der Größe des möglichen Leserkreises beim Einbezug von Freunden der Freunde als offensichtlich öffentlich zu werten ist, wäre ggf. anhand der Umstände des Einzelfalls zu prüfen.

4.20 Google – neue Datenschutzerklärung

Im Januar 2012 gab Google bekannt, seine bisherigen über 70 Datenschutzerklärungen zu den einzelnen Google-Diensten in einer einzigen für alle Dienste geltenden Datenschutzerklärung zusammenfassen zu wollen.

Seit dem 1. März 2012 gelten für Google-Nutzer die neuen Datenschutzbestimmungen, d. h. jeder, der einen Account bei Gmail, Google Docs, Google+, Picasa, Youtube oder einem der vielen anderen Dienste hat, ist von der Änderung betroffen. Alle Accounts eines Nutzers werden in einem zentralen Google-Account unter einem Namen und einem Profil zusammengefasst.

In den Nutzerprofilen sammelt Google Daten aus verschiedenen Quellen. Einerseits geben Nutzer bei der Erstellung eines Accounts oft persönliche Daten wie Name, Adresse oder Kreditkartennummer an. Andererseits werden aber auch Daten gesammelt, die bei der Nutzung der Google-Dienste anfallen. Welche konkreten Nutzungsdaten zu welchem Zweck erfasst werden, sollte in den neuen Bestimmungen zum Datenschutz eindeutig festgelegt sein. Das ist jedoch nicht der Fall. Die Formulierungen sind stattdessen sehr vage und beinhalten Begriffe wie „beispielsweise“, „gegebenenfalls“ und „möglicherweise“, sodass der Nutzer auch nach dem Lesen der Datenschutzerklärung nicht genau weiß, welche seiner Daten für welche Zwecke und wie lange gespeichert werden.

Die französische Datenschutzbehörde CNIL hat seit Anfang Februar 2012 im Auftrag der Artikel-29-Gruppe der Europäischen Datenschutzbehörden untersucht, inwieweit die neue Datenschutzerklärung von Google den Anforderungen des europäischen Datenschutzrechts genügt. Die Untersuchung der CNIL kam zu dem Ergebnis, dass die Datenschutzerklärung gegen die Verpflichtung des Unternehmens zu umfassender Transparenz bezüglich des Umgangs mit personenbezogenen Nutzerdaten verstoße. Zudem ist die pauschale Ermächtigung zur Erstellung umfassender diensteübergreifender Nutzerprofile und die fehlende Festlegung der Speicherdauer nicht mit den Anforderungen der EU-Datenschutzrichtlinie 95/46/EG vereinbar.

Die Bitte der CNIL, das Inkrafttreten der Datenschutzerklärung auszusetzen, wurde abgelehnt. Daraufhin forderte die CNIL Google Mitte März 2012 zu einer Stellungnahme bezüglich der Konformität der Datenschutzerklärung mit den Vorgaben der Europäischen Datenschutzrichtlinie auf. Die insgesamt 69 Fragen wurden jedoch nach Ansicht der Artikel-29-Gruppe nur unzureichend beantwortet.

Aufgrund der fehlenden Bereitschaft Googles, Maßnahmen zur Behebung der bestehenden Verstöße zu ergreifen, hat der Hamburgische Datenschutzbeauftragte Anfang Juli 2013 ein offizielles Verfahren gegen Google eingeleitet. Dieses ist Teil einer durch die CNIL koordinierten Aktion, an der Datenschutzbehörden mehrerer EU-Länder beteiligt sind. Ziel des Verfahrens ist die datenschutzkonforme Ausgestaltung der derzeitigen Verarbeitungspraxis bei Google.

In einem anderen Verfahren gegen Google hat der Bundesgerichtshof am 14. Mai 2013 entschieden, dass Nutzer die Löschung automatischer Suchvorschläge verlangen können, wenn sie ihre Persönlichkeitsrechte verletzt sehen (NJW 2013, 2348). Bei der automatischen Vervollständigung von Suchanfragen (Autocomplete-Funktion) werden die Begriffe er-

gänzt, die zuvor von anderen Nutzern im Zusammenhang mit dem gesuchten Begriff eingegeben wurden. Das birgt jedoch auch die Gefahr von Manipulationen, da so ganz bewusst positive wie negative Begriffe mit einem Suchwort verknüpft werden können.

4.21 Personenortung durch GPS

Aus den unterschiedlichsten Gründen stellen manche Detekteien Dritten, z. B. den Ehepartnern von Auftraggebern, mit GPS-Sendern nach. Diese handlichen Geräte, unbemerkt am Auto der Zielperson befestigt, können über das Mobilfunknetz im Minutentakt zeitgestempelte Angaben über die aktuelle geografische Position und die Bewegungsgeschwindigkeit an einen Empfänger senden. Mit der geeigneten Software können diese personenbezogenen Daten zu Bewegungsprotokollen und Kartendarstellungen zusammengestellt werden, um z. B. einen Ehepartner der Untreue zu überführen. Von den Akteuren wird dabei übersehen, dass diese Verfahrensweise nach § 44 i. V. m. § 43 Abs. 2 Nr. 3 BDSG grundsätzlich schlichtweg strafbar ist. Der Bundesgerichtshof (BGH) hatte sich mit diesem Thema befasst und eben diese Strafbarkeit explizit festgestellt (vgl. Urteil vom 4. Juni 2013, NJW 2013, 2530).

Ausnahmen hält der Bundesgerichtshof allenfalls bei starkem berechtigten Interesse – also in notwehrähnlichen Situationen, wie einem nicht anders abwehrbaren Angriff auf die berufliche Existenz – dann für hinnehmbar, wenn nicht durch andere, weniger belastende Methoden der Sachverhalt anderweitig aufgeklärt werden kann. In der Regel stellen §§ 28, 29 oder andere Vorschriften des BDSG keine ausreichende Erlaubnisnorm für die GPS-Ortung dar, da das allgemeine Persönlichkeitsrecht der überwachten Person überwiegt.

Ähnliches galt auch in einem anderen von einem Zivilsenat des BGH zu entscheidenden Fall: Der Kläger war zu nachehelichem Unterhalt verurteilt worden, wollte aber nachweisen, dass sich die geschiedene Ehefrau in einer verfestigten Lebensgemeinschaft befindet, was zu einem Wegfall ihres Unterhaltsanspruchs hätte führen können. Gerichtlich machte er seine Kosten für die GPS-Überwachung seiner geschiedenen Ehefrau i. H. v. über 3.700 € geltend. Hier stellte das Gericht fest, dass der Kläger zwar hätte Nachforschungen anstellen können, ob die geschiedene Ehefrau in einer verfestigten Lebensgemeinschaft lebe. Hierzu stünden ihm aber mildere Mittel als die der GPS-Ortung zur Verfügung. Denn diese ermöglicht eine lückenlose Überwachung aller Fahrten, egal ob sie aus privaten oder beruflichen Gründen erfolgen. Eine punktuelle persönliche Beobachtung z. B. in den Abendstunden hätte den erwünschten Nachweis ebenso erbringen können. Die mit Hilfe des GPS-Geräts erhobenen Daten stellten auch hier einen unzulässigen Eingriff in das Persönlichkeitsrecht der Beklagten dar. Das Beweisergebnis der Ortung sei daher gerichtlich nicht verwertbar gewesen und die Kosten dafür seien nicht erstattungsfähig (BGH, Beschluss vom 15. Mai 2013, NJW 2013, 2668).

Der Landesbeauftragte rät daher dringend vom Einsatz von GPS-Geräten ab. Selbst wenn man berechtigte Interessen zur Feststellung von Aufenthaltsorten unterstellt, stehen regelmäßig Mittel zur Verfügung, die einen deutlich geringeren Eingriff in das allgemeine Persönlichkeitsrecht darstellen. Derzeit befinden sich noch mehrere Einzelfälle in der Bearbeitung, bei denen sich die Frage stellt, inwieweit die Ortung mit Hilfe von GPS-Geräten eine Straftat oder eine Ordnungswidrigkeit darstellt.

5 Öffentliche Sicherheit, Einwohner- und Ausländerwesen

5.1 SOG LSA

In seinem X. Tätigkeitsbericht (Nr. 19.2) hat der Landesbeauftragte zum wiederholten Male darauf hingewiesen, dass das SOG LSA überarbeitungsbedürftig ist, weil die bestehende Rechtslage nicht mehr den Anforderungen entspricht, welche die Rechtsprechung zwischenzeitlich aufgezeigt hat. Das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt hat zu diesem Zeitpunkt eine Änderung des SOG LSA jedoch als nicht sachdienlich angesehen.

Im Januar 2012 wurde dem Landesbeauftragten dann erstmalig der Entwurf eines Vierten Gesetzes zur Änderung des SOG LSA durch das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt übersandt. Zu diesem Referentenentwurf nahm der Landesbeauftragte im Februar 2012 schriftlich Stellung. Im Mai 2012 erfolgte dann die Anhörung zum Gesetzentwurf der Landesregierung. Auch diese Gelegenheit zur Stellungnahme nahm der Landesbeauftragte mit einem Schreiben im Juni 2012 wahr, obwohl aus datenschutzrechtlicher Sicht zum Referentenentwurf kaum Veränderungen vorgenommen wurden. Die durch den Landesbeauftragten vorgetragenen Bedenken fanden keinen nennenswerten Eingang in die Überarbeitung vom Juli 2012.

In seiner Stellungnahme verwies der Landesbeauftragte insbesondere auf datenschutzrechtliche Bedenken hinsichtlich der Datenerhebung zur Eigensicherung (§ 16), der Datenerhebung durch Observation und Einsatz technischer Mittel (§ 17), der Datenerhebung durch Überwachung und Aufzeichnung der Telekommunikation (§ 17a), der Datenerhebung in informationstechnischen Systemen (§ 17b), der Aufzeichnung von Telefon- und Funkgesprächen (§ 23a), der Rasterfahndung (§ 31) und der Durchsuchung von Personen (§ 41). Zentrale Fragen bei dieser Änderung des SOG LSA waren die nach der Einführung der Befugnis der Polizei zur Datenerhebung durch Überwachung und Aufzeichnung der Telekommunikation in § 17a SOG LSA und zur Datenerhebung durch Quellen-Telekommunikationsüberwachung in § 17b SOG LSA. In beiden Fällen mangelte es an einer nachvollziehbaren Begründung zur Erforderlichkeit der Maßnahme. Der Bedarf an derartigen Überwachungsmaßnahmen mit Eingriffen auch in informationstechnische Systeme wird nicht konkretisiert. Die Gesetzesbegründung (LT-Drs. 6/1253) bleibt den Nachweis schuldig, dass und in welchem Umfang die Durchführung von Telekommunikationsüberwachungs- und Quellen-Telekommunikationsüberwachungsmaßnah-

men durch die Polizei zur Aufgabenwahrnehmung zwingend ist. Neben diesen grundsätzlichen Bedenken hat der Landesbeauftragte sich auch zur Ausgestaltung der Normen geäußert.

Während der parlamentarischen Anhörung wurden darüber hinaus die Kennzeichnungspflicht für Polizisten und die Untersuchung von Personen auf besonders gefährliche Krankheitserreger thematisiert. Der Landesbeauftragte brachte sich in diese Diskussion im Rahmen der mündlichen Anhörung ein. Die Kennzeichnungspflicht fand letztendlich keinen Eingang in das Gesetz, die Regelung zur Untersuchung von Personen schon. Hinsichtlich der Kennzeichnungspflicht muss der Vollständigkeit halber an dieser Stelle darauf hingewiesen werden, dass es eine solche faktisch dennoch gibt. Durch Bekleidungserlass des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt vom August 2009 ist unter der Überschrift „Namensschild“ geregelt, dass das Tragen eines Namensschildes auf freiwilliger Basis erwünscht ist. Das Vertrauen in die Polizei werde durch diese Offenheit, die Transparenz des Handelns und die Fortsetzung des weiteren Ausbaus einer bürgerorientierten Polizeiarbeit gestärkt. Diese Art der Freiwilligkeit ist allerdings relativ. Beim Einsatz von Polizeiverbänden soll zwar auf das Namensschild verzichtet werden. Gleichwohl wurde die datenschutzgerechte Lösung der Vergabe von Nummern nicht berücksichtigt.

Eine nicht akzeptable Feststellung trifft das Ministerium auf Seite 44 der Gesetzesbegründung (LT-Drs. 6/1253): Danach soll der polizeiliche Einsatz eines IMSI-Catchers zur Ermittlung des Standortes eines Mobiltelefons oder der Ermittlung der Geräte- und Kartennummer bereits ein Anwendungsfall der allgemeinen, generalklauselartigen Befugnis zum Einsatz technischer Mittel zur Datenerhebung durch Observation gem. § 17 Abs. 2 SOG LSA sein; der Schutzbereich des Art. 10 GG sei nicht berührt. Dies reicht rechtsstaatlich keineswegs aus, wie auch die Parallelsituation bzw. -regelung für den Verfassungsschutz in § 17a Abs. 6 VerfSchG-LSA deutlich macht. Dort wurde im Übrigen auch ein möglicher Grundrechtseingriff in Art. 10 GG mitzitiert (vgl. Nr. 8.4).

Nachdem das Vierte Gesetz zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt Ende März 2013 (GVBl. LSA S. 145 ff.) im Wesentlichen unverändert beschlossen worden war, erreichte den Landesbeauftragten Anfang Mai 2013 erneut ein Gesetzentwurf zur Änderung des SOG LSA. Es handelte sich um den Entwurf eines Gesetzes zur Neuregelung der Erhebung von telekommunikations- und telemedienrechtlichen Bestandsdaten. Mit diesem Gesetzentwurf sollten die Vorgaben des Bundesverfassungsgerichtes aus seiner Entscheidung zum Telekommunikationsgesetz (1 BvR 1299/05 vom 24. Januar 2012, NJW 2012, 1419) umgesetzt werden. Gegenstand der Verfassungsbeschwerde waren insbesondere die Verfassungsmäßigkeit der Regelungen über die Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten zur Speicherung bestimmter (Bestands-)Daten sowie zur Beauskunftung dieser Daten im Wege des automatisierten oder manuellen Auskunftsverfahrens. Eingehend mit der Entscheidung des Bundesverfassungsgerichtes befasst sich Nr. 4.13.

Um die Möglichkeiten des Auskunftsverfahrens über Juni 2013 hinaus nutzen zu können, musste eine entsprechende Rechtsgrundlage im SOG LSA geschaffen werden. Zu diesem Zweck wurde mit dem Gesetz zur Neuregelung der Erhebung von telekommunikations- und telemedienrechtlichen Bestandsdaten u. a. ein zusätzlicher § 17a – Erhebung von Telekommunikations- und Telemedienbestandsdaten – in das SOG LSA eingefügt.

In seiner Stellungnahme vom Mai 2013 zum Gesetzentwurf wies der Landesbeauftragte darauf hin, dass die Eingriffsschwelle für Maßnahmen nach der neuen Regelung zwar den Maßgaben des Bundesverfassungsgerichtes entspricht, es allerdings auch festgestellt hat, dass diese Schwelle freilich niedrig sei und den Gefahrenverdacht mit umfasst. Die Maßgaben des Gerichts schließen für den Landesgesetzgeber jedoch nicht aus, die Eingriffsschwelle höher als das bundesverfassungsrechtlich festgestellte Mindestmaß festzulegen. Aus datenschutzrechtlicher Sicht ist die Orientierung am Mindeststandard zwar zulässig, aber infolge des Fehlens einer eigenen Wertung in diesem Punkt der Begründung des Gesetzentwurfes nicht angemessen. Darüber hinaus hat der Landesbeauftragte erneut die Aufnahme einer Evaluierungsklausel für neu eingeführte Eingriffsbefugnisse eingefordert. Nur so können die Auswirkungen neuer Befugnisse auf den Normadressaten überhaupt eingeschätzt werden. Den Gesetzgeber trifft nach der Rechtsprechung des Bundesverfassungsgerichtes die Verpflichtung, die informationstechnischen Entwicklungen zu beobachten und zugunsten eines effektiven Grundrechtsschutzes rechtliche Vorkehrungen mittels Datenschutzes durch Verfahren und Technik vorzusehen. Auf die diesbezüglichen Ausführungen des Landesbeauftragten in seinem X. Tätigkeitsbericht (Nr. 1.1) und die Stellungnahme der Landesregierung dazu wird an dieser Stelle verwiesen. Die Landesregierung hat mit ihrer Stellungnahme eingeräumt, dass die Evaluation von Eingriffsgesetzen nötig sei, verzichtet hier aber erneut darauf.

Der Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt hat im September 2013 seine Beschlussempfehlung an den Landtag von Sachsen-Anhalt (LT-Drs. 6/2341 neu) abgegeben. Mit den Änderungen am Regierungsentwurf (LT-Drs. 6/2219) wurde zumindest die parlamentarische Kontrolle für Bestandsdatenauskünfte gestärkt und das ursprünglich vorgesehene rückwirkende Inkrafttreten des Gesetzes ausgeschlossen (Gesetz zur Neuregelung der Erhebung von telekommunikations- und telemedienrechtlichen Bestandsdaten vom 10. Oktober 2013, GVBl. LSA S. 494).

5.2 Geldwäscheprävention

Im Dezember 2011 hat der Bundestag das Gesetz zur Optimierung der Geldwäscheprävention (BGBl. I S. 2959) verabschiedet.

Der Gesetzentwurf sah durch den Verzicht auf Schwellenwerte zunächst vor, dass z. B. auch Verkäufer von Prepaid-Karten verpflichtet sind, Kunden bei deren Erwerb zu identifizieren. Aus datenschutzrechtlicher Sicht

ist eine solche verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung unverhältnismäßig. Deshalb wandte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung vom September 2011 „Anonymes elektronisches Bezahlen muss möglich bleiben!“ (**Anlage 8**) an den Gesetzgeber und wies u. a. darauf hin, dass auch europarechtlich diese umfassende und generelle Identifizierungspflicht nicht geboten sei (vgl. Nr. 13.1.5).

In der letztendlich beschlossenen Fassung des Gesetzes wurden die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geäußerten Bedenken teilweise aufgegriffen und ein Schwellenwert eingeführt. Das Geldwäschegesetz sieht eine Identifizierungspflicht erst ab einem Wert von 100 Euro pro Monat vor.

Die Gesetzesnovelle hat jedoch trotz dieser Entwicklung zu einer Verschärfung und Ausweitung der Sorgfalts- und Meldepflichten, zur Absenkung der Verdachtsstufen und zur Erweiterung des Verpflichtetenkreises geführt. Die Datenerhebungs- und Datenspeicherungspflichten der Verpflichteten wurden ausgeweitet, die Bußgeldandrohungen bei Verletzung der Sorgfaltspflichten erhöhen zudem den Druck auf die Verpflichteten.

Bei den politisch exponierten Personen (PEP) greifen zudem verstärkte Sorgfaltspflichten ein. In diesem Zusammenhang ist die Nutzung von „PEP-Listen“ datenschutzrechtlich kritisch zu betrachten. Auf diesen Listen werden von kommerziellen, oftmals auch von ausländischen Anbietern Informationen (Name, Geburtsdatum, Nationalität, Wohnort, gegenwärtige Position, Foto, …) zusammengestellt. Bei ausländischen Anbietern entzieht sich die Erfassung auf diesen Listen einer Kontrolle durch Datenschutzbehörden. Zwar besteht keine Verpflichtung zur Nutzung solcher kommerziellen Listen, in der Praxis werden sie aber genutzt.

Im Februar 2013 wurde durch das Gesetz zur Ergänzung des Geldwäschegesetzes (BGBl. I S. 268) der Kreis der Verpflichteten um die künftig in Deutschland legal operierenden Veranstalter und Vermittler von Glücksspielen im Internet erweitert. Für diesen Bereich wurden zudem spezifische Sicherungsmaßnahmen eingeführt. So sind z. B. angemessene Datenverarbeitungssysteme zu betreiben, die unerlaubtes Zusammenwirken von Spielern erkennen und die Identifizierung vor der Teilnahme an Glücksspielen vorsehen.

5.3 Anti-Terror-Maßnahmen

Infolge der Anschläge vom 11. September 2001 hat der Gesetzgeber mit dem Terrorismusbekämpfungsgesetz und dem Terrorismusbekämpfungsergänzungsgesetz befristet Befugnisse eingeräumt, die es den Polizeien, Strafverfolgungsbehörden und Nachrichtendiensten ermöglichen sollten, den internationalen Terrorismus besser als bisher zu bekämpfen. Diese vor dem Hintergrund der aktuellen Ereignisse und unter Zeitdruck erlassenen Gesetze bedürfen einer Evaluation, die die Befugnisse auf ihren Nutzen und ihre Verhältnismäßigkeit hin überprüft. Diese Forderung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit

ihrer Entschließung vom September 2011 „Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick“ (**Anlage 3**) aufgestellt bzw. konkretisiert. Die Konferenz fordert eine umfassende und unabhängige wissenschaftliche Evaluation, und nicht den Einsatz einer Regierungskommission. Eine umfassende Evaluation hätte die Auswirkungen der bestehenden Sicherheitsgesetze auch und vor allem in deren Zusammenwirken zu untersuchen. Die Evaluierung z. B. des Terrorismusbekämpfungsergänzungsgesetzes, wofür das Bundesministerium des Innern 2011 lediglich externe Methodenberatung einholte, wird den formulierten Anforderungen jedenfalls nicht gerecht.

Neben den Terrorismusbekämpfungsgesetzen wurden auch mit den Gesetzen zur Antiterrordatei und zur Verbesserung der Bekämpfung des Rechtsextremismus die Anti-Terror-Maßnahmen ausgebaut. Mit der **Antiterrordatei** wurde eine Verbunddatei geschaffen, die von Polizeien und Nachrichtendiensten gemeinsam genutzt wird und die Bekämpfung des Terrorismus verbessern soll. Im Aufbau angelehnt an das Antiterrordateigesetz wurde zur Bekämpfung des Rechtsextremismus das Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus als Folge der Straftaten des Nationalsozialistischen Untergrundes erlassen. Damit wurde eine weitere Verbunddatei installiert, durch die der Informationsfluss zwischen Polizeien und Nachrichtendiensten erweitert wird. Gegen beide Gesetze bestanden bzw. bestehen verfassungsrechtliche Bedenken.

In Bezug auf die Antiterrordatei hat das Bundesverfassungsgericht mit seiner Entscheidung vom 24. April 2013 (ZD 2013, 328) zwischenzeitlich festgestellt, dass verschiedene Regelungen des Antiterrordateigesetzes verfassungswidrig sind. Insbesondere die Regelungen zu Kontaktpersonen und Unterstützern wurden durch das Bundesverfassungsgericht als mit dem Grundgesetz nicht vereinbar bewertet. Auf derartige verfassungsrechtliche Bedenken hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit ihrer Entschließung im Oktober 2006 „Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten“ hingewiesen. Die Rechtsextremismusdatei, die nach dem Vorbild der Antiterrordatei entstand, muss sich nach dieser Entscheidung des Bundesverfassungsgerichtes an den damit aufgestellten Grundsätzen messen lassen. Mit seiner Entscheidung hat das Bundesverfassungsgericht auch verdeutlicht, dass Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendienste ermöglichen, gesteigerten verfassungsrechtlichen Anforderungen hinsichtlich des Grundrechts auf informationelle Selbstbestimmung unterliegen. Aus dem Grundrecht folgt ein **informationelles Trennungsprinzip**, das diesen Austausch nur ausnahmsweise zulässt. Das Gericht betont angesichts der Verkürzung der Betroffenenrechte durch die geringe Transparenz der Maßnahmen die Notwendigkeit der Kompensation durch parlamentarische Kontrolle und effektive Datenschutzaufsichtskontrolle (dies unterstreicht auch der Bundestag in seinem Beschluss vom 14. Juni 2013, BT-Drs. 17/13936, Nr. 5).

Ebenfalls als Ausfluss der Terrorismusbekämpfung ist die Bildung verschiedenster Sicherheitszentren auf Bundes- und Landesebene anzusehen. Über das in Sachsen-Anhalt eingerichtete Gemeinsame Informations-

und Auswertungszentrum islamistischer Terrorismus hat der Landesbeauftragte wiederholt – zuletzt in seinem IX. Tätigkeitsbericht unter Nr. 25.3 – berichtet. Seine an der Struktur geäußerten Bedenken hält der Landesbeauftragte weiterhin aufrecht. Auf Bundesebene sind in den letzten Jahren zusätzliche Sicherheitszentren entstanden, umgebildet oder zusammengelegt worden. Den Überblick zu behalten ist dabei wahrscheinlich auch hinsichtlich der jeweils wahrzunehmenden Aufgaben nicht einfach. So wurden – um nur einige zu nennen – das Gemeinsame Terrorismusabwehrzentrum (GTAZ), das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ), das Gemeinsame Analyse- und Strategiezentrum illegale Migration (GASIM), das Gemeinsame Internetzentrum (GIS) und das Gemeinsame Abwehrzentrum gegen Rechtsextremismus (GAR) errichtet. Allen Zentren ist eine gemeinsame Struktur gegeben. Genau darin besteht auch die datenschutzrechtliche Gefahr.

Bei aller Verbesserung der Zusammenarbeit zwischen Polizei und Nachrichtendiensten darf das Trennungsgebot nicht aus dem Auge verloren werden. Der Landesbeauftragte hat dazu bereits in seinem VIII. Tätigkeitsbericht (Nr. 24.2) ausführlich Stellung genommen (vgl. unten Nr. 8.1).

5.4 Risikomanagement für besonders rückfallgefährdete Sexualstraftäter

In seinem IX. Tätigkeitsbericht hat der Landesbeauftragte unter Nr. 18.10 über den gemeinsamen Erlass „Maßnahmen zur Verbesserung des Schutzes der Bevölkerung vor Straftaten von haftentlassenen rückfallgefährdeten Sexualstraftätern“ berichtet. Die im Jahr 2008 veröffentlichte Fassung des Erlasses war mit dem Landesbeauftragten abgestimmt.

Im Jahr 2012 kam das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt auf den Landesbeauftragten mit der Mitteilung zu, dass der Erlass aus dem Jahr 2008 überarbeitet werden soll. Sachgerechte Maßnahmen sollten so noch effektiver als bislang umgesetzt werden können. Im Kern der Überlegungen stand die Einrichtung einer Zentralstelle, die Maßnahmeempfehlungen an die für den Wohnort zuständige Polizeidirektion ausspricht. Darüber hinaus sollten die Informationsbeziehungen zwischen der Polizei und der Justiz sowie innerhalb der Polizei geregelt werden.

An einem Freitagnachmittag im Oktober 2012 erreichte den Landesbeauftragten dann eine erste überarbeitete Fassung des Erlasses mit dem Hinweis, dass eine Schlusszeichnung bereits am darauffolgenden Dienstag vorgesehen sei. Eine inhaltliche Prüfung war unter diesen zeitlichen Vorgaben ausgeschlossen. Zur Schlusszeichnung kam es nicht, sodass dem Landesbeauftragten zwei Wochen später donnerstags eine überarbeitete Fassung übersandt wurde, bei der die Schlusszeichnung wiederum für den darauffolgenden Dienstag vorgesehen war. Am Nachmittag desselben Tages erreichte den Landesbeauftragten dann eine nochmals veränderte Fassung des Erlasses. Der Landesbeauftragte machte daraufhin das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt schriftlich da-

rauf aufmerksam, dass es ihm unter diesen engen zeitlichen Vorgaben nicht möglich sei, eine inhaltliche Prüfung vorzunehmen und eine Stellungnahme abzugeben. Die Art und Weise der Beteiligung in diesem Verfahren erachtete der Landesbeauftragte als mit den gesetzlichen Vorgaben dazu als nicht vereinbar. Inhaltlich wies der Landesbeauftragte auf zwei Aspekte – Aufgaben der gemeinsamen Zentralstelle und Gestaltung von Fallkonferenzen – hin, gegen die datenschutzrechtlich zunächst Bedenken bestanden. Eine Woche später ging beim Landesbeauftragten erneut eine überarbeitete Fassung des Erlasses ein.

Nach einer eingehenden Prüfung wurde die Thematik drei Wochen nach Vorlage der letzten Entwurfsfassung beim Landesbeauftragten mit dem Ministerium für Inneres und Sport des Landes Sachsen-Anhalt besprochen und wiederum zwei Tage später übersandte der Landesbeauftragte seine schriftliche Stellungnahme. Der Landesbeauftragte wies darauf hin, dass eine stärkere Verzahnung von Polizei und Justiz im Bereich des Risikomanagements für besonders rückfallgefährdete Sexualstraftäter aus datenschutzrechtlicher Sicht die Gefahr einer unzulässigen Vermischung der Kompetenzen und der zur Aufgabenwahrnehmung jeweils erhobenen personenbezogenen Daten birgt.

Zur Vermischung der Kompetenzen führte der Landesbeauftragte aus, dass Ziel der Führungsaufsicht die Resozialisierung von Straftätern mit ungünstiger Sozialprognose und die Verhinderung weiterer Straftaten ist. Eine inhaltliche Überschneidung mit gefahrenabwehrrechtlichen Maßnahmen seitens der Polizei findet sich – wenn überhaupt – in einem Teilbereich der Aufgaben der Führungsaufsicht. Aufsichtsstelle und Bewährungshelfer sollen der verurteilten Person helfend und betreuend zur Seite stehen. Die polizeiliche Aufgabe der Gefahrenabwehr ist dagegen nicht auf die verurteilte Person, sondern auf den Schutz der Allgemeinheit gerichtet.

Hinsichtlich der Vermischung personenbezogener Daten trug der Landesbeauftragte vor, dass eine Verstärkung der Zusammenarbeit von Polizei und Justiz in einer Gemeinsamen Zentralstelle beim Landeskriminalamt klar definierter Weisungsverhältnisse und Übermittlungskompetenzen bedarf. Polizei und Justiz dürfen jeweils nur in ihren eigenen Unterstellungsverhältnissen agieren und die gegenseitige Übermittlung personenbezogener Daten muss konsequent an der Erforderlichkeit der Daten zur Aufgabenwahrnehmung des jeweils anderen ausgerichtet sein. Bei der Gemeinsamen Zentralstelle beim Landeskriminalamt dürfen personenbezogene Daten zu Betroffenen nur insoweit zusammengeführt werden, als sie für die Aufgabenwahrnehmung aller Beteiligten erforderlich sind. Darüber hinaus erscheint das Anlegen einer Datenbank bzw. Datensammlung im Verantwortungsbereich der Polizei, die personenbezogene Daten enthält, die zur polizeilichen Aufgabenwahrnehmung nicht erforderlich sind, aber alle Erkenntnisse zu einer bestimmten Person bündeln sollen, als datenschutzrechtlich nicht vertretbar.

In der letztendlich schlussgezeichneten und am 29. April 2013 veröffentlichten Fassung (MBl. LSA S. 207) wurden die Bedenken des Landes-

beauftragten nur teilweise berücksichtigt. Es wird auch Kontrollen des Landesbeauftragten vorbehalten sein, die datenschutzgerechte Umsetzung der Erlassregelungen bei den Beteiligten zu begleiten.

Im August 2013 hat das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt dem Landesbeauftragten doch noch den Entwurf von Festlegungen für ein automatisiertes Verfahren für das Verfahrensverzeichnis zur Errichtung einer Datei „Risikomanagement für besonders rückfallgefährdete Sexualstraftäter im Land Sachsen-Anhalt“ vorgelegt.

5.5 Datenübermittlung an Fußballvereine

Im Dezember 2011 hat sich ein Petent mit der Bitte an den Landesbeauftragten gewandt, die datenschutzrechtliche Zulässigkeit einer vermuteten Datenübermittlung der Polizei an einen Fußballverein zu überprüfen.

Der Petent hatte Post bekommen vom Stadionverbotsbeauftragten des Fußballvereins. Dieser teilte mit, dass er die Erteilung eines bundesweiten Betretensverbots für Stadien und Hallen prüfe. Berufen hat sich der Stadionverbotsbeauftragte auf Informationen über einen Vorfall, der sich unmittelbar vor einem Fußballspiel des Vereins ereignet hat und wegen dem die Polizei eine Anzeige gegen den Petenten wegen Landfriedensbruchs und Raubes erstattet hatte. Der Petent wollte nun überprüft wissen, ob die Übermittlung dieser Daten durch die Polizei an den Fußballverein zulässig war.

Der Landesbeauftragte hat die zuständige Polizeidirektion um Stellungnahme gebeten. Im Ergebnis der Bewertung konnte der Landesbeauftragte feststellen, dass die Übermittlung der personenbezogenen Daten durch die Polizei an den Fußballclub erfolgte und diese Übermittlung dem Grunde nach zulässig war.

Nach § 28 Abs. 1 SOG LSA kann die Polizei personenbezogene Daten an nichtöffentliche Stellen, wie sie ein Fußballverein ist, übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben, zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder zur Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

Die Polizei hatte den Familiennamen des Petenten und eine Kopie der Anzeige an den Fußballverein übermittelt. Die Datenübermittlung an den Verein erfolgte zur Erfüllung polizeilicher Aufgaben. Zu diesen Aufgaben gehört im Rahmen der Gefahrenabwehr auch die Verhütung zu erwartender Straftaten (§ 2 Abs. 1 SOG LSA). Der Petent war nach Auskunft der Polizei nicht nur an besagtem Tag im Zusammenhang mit Auseinandersetzungen polizeilich in Erscheinung getreten, sondern der Polizei bereits auf Grund fußballbezogener strafrechtlicher Ermittlungsverfahren aus der Vergangenheit bekannt. Ein bundesweites Stadionverbot war gegen den Petenten bereits in der Vergangenheit verhängt worden. Aus Sicht der Polizei war die Besorgnis weiterer vom Petenten ausgehender Störungen im Zusammenhang mit Fußballveranstaltungen gegeben. Zweck eines Stadi-

onverbotes ist es, potentielle Störer auszuschließen, die die Sicherheit und den reibungslosen Ablauf von Großveranstaltungen wie einem Liga-Fußballspiel gefährden können. Die Störungen beschränken sich hierbei nicht ausschließlich auf den Stadionbereich, sondern schließen Störungen bei An- und Abreisen zu den Veranstaltungen – insbesondere bei einem Aufeinandertreffen mit rivalisierenden Fans – mit ein. Die Verhängung eines Stadionverbotes erschien der Polizei eine verhältnismäßige Maßnahme zu sein, um die vom Petenten als potentiellen Störer ausgehenden Gefahren abzuwehren.

Da ein Stadionverbot aber nicht von der Polizei selbst sondern vielmehr vom betreffenden Verein auszusprechen ist, war es zur Umsetzung der als verhältnismäßig angesehenen Maßnahme erforderlich, die personenbezogenen Daten des Petenten an den Fußballverein zu übermitteln.

Die Auffassung der Polizei, dass die Datenübermittlung zur polizeilichen Aufgabenwahrnehmung im Sinne des § 28 Abs. 1 SOG LSA dem Grunde nach erforderlich war, teilte der Landesbeauftragte. Lediglich die Frage nach dem Umfang der Datenübermittlung bedurfte noch einer Klärung mit der Polizeibehörde.

Für einzelne der übermittelten personenbezogenen Daten (Geburtsort, Geburtsland, Staatsangehörigkeit und Familienstand) konnte die Polizei nicht erklären, warum sie für die Erteilung eines Stadionverbotes erforderlich seien. Es wurde deshalb veranlasst, dass der Fußballverein diese Angaben zum Petenten löschen muss und dass in Zukunft diese Daten durch die Polizei nicht mehr an Fußballvereine übermittelt werden.

5.6 Öffentlichkeitsfahndung in sozialen Netzwerken

Die zunehmende Bedeutung sozialer Netzwerke im Internet macht dieses Medium auch für die öffentliche Fahndung nach Personen im Rahmen von Ermittlungsverfahren interessant. Über soziale Netzwerke können Ermittlungsbehörden kurzfristig Mengen von Menschen erreichen, die sie mit klassischen Methoden nicht zu erreichen imstande sind. Diese rein praktische Sicht auf die Öffentlichkeitsfahndung blendet aber aus, dass die Personenfahndung im Internet ein sehr schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht ist.

Dem Grunde nach darf die Polizei bei der Suche nach tatverdächtigen Personen oder wichtigen Zeugen die Öffentlichkeit einschalten. Dies gilt aber nur, wenn wegen einer erheblichen Straftat ermittelt wird und die Ermittlung des Aufenthaltes einer Person auf andere Weise erheblich weniger Erfolg verspricht oder wesentlich erschwert wäre. Die Anordnung einer solchen Fahndung ist Richtern vorbehalten, sofern kein Haftbefehl vorliegt (§§ 131 bis 131c StPO).

Eine Öffentlichkeitsfahndung im Internet ist wegen der Schwere des Eingriffs nur in Ausnahmefällen in Betracht zu ziehen. Der Eingriff ist bereits bei einer Veröffentlichung der Fahndung ausschließlich auf den Internetseiten der Polizei von besonderem Gewicht. Bei der Einbeziehung privat

betriebener Internetseiten, wie es bei sozialen Netzwerken der Fall ist, stellt sich die Situation noch problematischer dar. Bislang ist nach Nr. 3.2 der Anlage B der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) die Einschaltung privater Internetanbieter ausgeschlossen (vgl. VII. Tätigkeitsbericht, Nr. 18.6).

Trotzdem sollen nach einem Beschluss der Innenministerkonferenz vom 30. Mai bis 1. Juni 2012 bundesweite Standards als Voraussetzungen und Rahmenbedingungen für die Nutzung von sozialen Netzwerken auch bei polizeilichen Fahndungen im Internet entwickelt werden. Diesen Beschluss haben die Datenschutzbeauftragten des Bundes und der Länder zum Anlass genommen, mit einem gemeinsamen Schreiben an die Vorsitzenden der Innenminister- und Justizministerkonferenz darauf hinzuweisen, welche Gefährdungen von der Fahndung im Internet an sich und von der Fahndung in sozialen Netzwerken für die Rechte der Betroffenen ausgehen. Die Justizministerkonferenz hat durch Beschluss vom November 2012 den Strafrechtsausschuss gebeten, das Bestehen etwaigen Handlungsbedarfs in Bezug auf die Nutzung sozialer Netzwerke für die Aufklärung von Straftaten zu prüfen. Es deutet sich eine Öffnung der RiStBV an.

Öffentlichkeitsfahndungen im herkömmlichen Sinn erfolgten über traditionelle Medien wie Printmedien, Fernsehen und Radio. Sie waren dadurch lokal oder regional begrenzt. Wird nun aber heute eine Veröffentlichung von Daten zu einer Person im Internet vorgenommen, hat dies eine weltweite Verbreitung der Daten zur Folge. Ein Schutz gegen Weiterverbreitung ist nicht vorhanden, eine Löschung aus dem Internet ist nicht möglich. Neben diesen datenschutzrechtlich bereits schwer auflösbaren Problemen kommen bei der Einbeziehung privat betriebener Internetseiten, also auch sozialen Netzwerken, noch zusätzliche hinzu. Mit der Veröffentlichung von Fahndungen in sozialen Netzwerken gelangen diese Daten auf Server des jeweiligen Betreibers und verlassen insoweit den Herrschaftsbereich der Ermittlungsbehörden. Bei der Berichtigung oder Löschung dieser Veröffentlichungen in sozialen Netzwerken sind die Ermittlungsbehörden dann auf die Mitwirkung privater Betreiber angewiesen, die ggf. noch nicht einmal dem deutschen Datenschutzrecht unterliegen, weil die Firmensitze im Ausland angesiedelt sind. Die Durchsetzung der Interessen der Ermittlungsbehörden dürfte sich in Fällen, in denen der private Betreiber nicht freiwillig kooperiert, durchaus schwierig gestalten. Personenbezogene Daten sollten daher in der Hand der Behörden bleiben.

Alles in allem birgt die Nutzung sozialer Netzwerke zu Zwecken der Öffentlichkeitsfahndung ein erhebliches Gefährdungspotential. Aber nicht nur die Frage nach einer datenschutzgerechten Ausgestaltung der Öffentlichkeitsfahndung ist in Bezug auf soziale Netzwerke zu stellen. Die Nutzung sozialer Netzwerke wirft auch ansonsten verschiedene Fragen rund um den Datenschutz auf. Der Bedeutung dieses Mediums ist sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder durchaus bewusst und hat mit ihrer Entschließung „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor“ vom März 2013 (**Anlage 25**) eine Anleitung zu mehr datenschutzgerechter Nutzung initiiert.

In Sachsen-Anhalt werden soziale Netzwerke derzeit nicht für die Öffentlichkeitsfahndung genutzt.

5.7 Glücksspielrecht

In seinem X. Tätigkeitsbericht (Nr. 10.3) hat der Landesbeauftragte sich zur Änderung des Spielbankgesetzes im Jahr 2009 geäußert. Seine damals im Gesetzgebungsverfahren vorgebrachten Bedenken gegen einzelne Regelungen fanden nicht vollumfassend Eingang in das letztendlich im Dezember 2009 veröffentlichte Gesetz.

Ende Dezember 2011 wurde dem Landesbeauftragten Gelegenheit gegeben, sich zum Entwurf eines Zweiten Glücksspielrechtsänderungsgesetzes zu äußern. Mit dem Zweiten Glücksspielrechtsänderungsgesetz sollten das Glücksspielgesetz und das Spielbankgesetz des Landes Sachsen-Anhalt geändert werden. In seiner Stellungnahme vom Januar 2012 trug der Landesbeauftragte seine Bedenken hinsichtlich der getroffenen Regelungen gegenüber dem Ministerium für Inneres und Sport vor.

Zum Glücksspielgesetz des Landes Sachsen-Anhalt wurden die Regelungen zur Sperrdatei (§ 14) und zur Offenbarungsbefugnis (§ 17a) als datenschutzrechtlich nicht vertretbar angesehen. Hinsichtlich der Sperrdatei blieben die Fragen nach der Dauer der Speicherung und der Form des Speicherns offen. Darüber hinaus waren die Informationspflicht über Grund und Dauer einer Spielersperre und die Unterrichtung zur Übernahme einer Spielersperre in die Sperrdatei datenschutzrechtlich unzureichend ausgestaltet. Zur Offenbarungsbefugnis musste festgestellt werden, dass die Formulierung „der Durchführung eines Verfahrens dient“ dem Bestimmtheitserfordernis an eine Datenübermittlungsbefugnis nicht gerecht wird.

Das Spielbankgesetz musste der Landesbeauftragte insoweit als datenschutzrechtlich unzulänglich ansehen, als es Regelungen zur Besucherdatei (§ 7) und zu Videoüberwachung (§ 8) traf. In die Besucherdatei sollten zukünftig zusätzlich zu den bisherigen Angaben auch die „Staatsangehörigkeit, Art, Nummer und ausstellende Behörde des amtlichen Ausweises“ aufgenommen werden. Die Erforderlichkeit dieser personenbezogenen Daten wurde aber nicht erläutert. Auch in Bezug auf die Videoüberwachung wurde der Umfang grundlegend erweitert, eine Begründung hinsichtlich der Erforderlichkeit gab es aber nicht.

Mit dem letztendlich dem Landtag vorgelegten Gesetzentwurf (LT-Drs. 6/914) eines Zweiten Glücksspielrechtsänderungsgesetzes wurden nur einige der durch den Landesbeauftragten vorgebrachten Bedenken ausgeräumt. So wurde zum Glücksspielgesetz geregelt, dass die Informationspflicht und die Unterrichtung jeweils schriftlich gegenüber dem Betroffenen erfolgen müssen. Zur Offenbarungsbefugnis – die im überarbeiteten Entwurf dann Mitteilungsbefugnis hieß – wurde vorgesehen, dass eine Datenübermittlung nur erfolgen darf, wenn die Übermittlung zur Durchführung eines Verfahrens in Steuersachen erforderlich ist. Die Fragen nach der Dauer der Speicherung und der Form des Speicherns blieben allerdings

auch mit diesem überarbeiteten Gesetzentwurf offen. Die Regelung zur Videoüberwachung im Spielbankgesetz wurde zwar überarbeitet und ist in ihrer letztendlichen Ausgestaltung datenschutzrechtlich nicht zu beanstanden, die erforderliche Begründung zur Ausweitung der Videoüberwachung wurde aber nicht mehr ergänzt.

Zudem wurde mit dem in den Landtag eingebrachten Gesetzentwurf ein bis dahin nicht mit dem Landesbeauftragten abgestimmtes Spielhallengesetz vorgelegt. Auch für Spielhallen ist eine Spielersperre (§ 7) vorgesehen. Die verhängten Spielersperren sollen in einer Sperrliste erfasst werden. Dazu sollen u. a. auch Lichtbilder der Betroffenen gespeichert werden. Die Erforderlichkeit einer solchen Maßnahme wurde aber nicht begründet.

Somit blieben für den Landesbeauftragten aus datenschutzrechtlicher Sicht verschiedene Fragestellungen offen, was er in seiner Stellungnahme gegenüber dem Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt im Mai 2012 auch nochmals zum Ausdruck brachte.

Der Landesbeauftragte wird die Umsetzung der neu gefassten Regelungen (Gesetz vom 25. Juni 2012, GVBl. LSA S. 691) in der Praxis beobachten und so eventuelle datenschutzrechtliche Defizite erkennen und benennen.

5.8 Nationales Waffenregister

Alle EU-Mitgliedstaaten sind nach der europäischen Waffenrichtlinie (2008/51/EG) verpflichtet, bis spätestens 31. Dezember 2014 ein computergestütztes Waffenregister auf nationaler Ebene einzurichten und allen zuständigen Behörden Zugang zu den darin gespeicherten Daten zu gewähren. Mit dem Nationalen-Waffenregister-Gesetz vom 25. Juni 2012 wurde die Einführung des Nationalen Waffenregisters für die Bundesrepublik Deutschland bis zum Ende des Jahres 2012 beschlossen (BGBl. I S. 1366).

Die gut 500 Waffenbehörden bundesweit waren nach dem Nationalen-Waffenregister-Gesetz verpflichtet, ihre Daten bis Ende Dezember 2012 in das Nationale Waffenregister, welches beim Bundesverwaltungsamt in Köln geführt wird, einzupflegen. Eine Waffenbehörde aus Sachsen-Anhalt gehörte auch zu den Projektteilnehmern, die bereits am Probebetrieb des Nationalen Waffenregisters beteiligt waren.

Der Landesbeauftragte hat sich im April 2013 vor Ort bei einer Waffenbehörde über den Stand der Umsetzung des Nationalen-Waffenregister-Gesetzes informiert. Im Ergebnis konnte er feststellen, dass die bisherige Umsetzung zunächst nicht zu beanstanden ist. Allerdings blieben verschiedene Fragen insbesondere zur IT-Sicherheit offen, weil noch nicht alle Bereiche des Nationalen Waffenregisters im Detail durchdrungen wurden. Der Landesbeauftragte hat sich weitergehende Informationen erbeten und wird auch die Einbindung anderer Behörden des Landes, die Zugang zum Nationalen Waffenregister haben, im Blick behalten.

5.9 Meldewesen

5.9.1 Bundesmeldegesetz

In seinem X. Tätigkeitsbericht hat der Landesbeauftragte unter Nr. 6.3 über den Gesetzentwurf zur Fortentwicklung des Meldewesens berichtet.

Die Bundesregierung hatte dem Deutschen Bundestag den Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) vom 16. November 2011 (BT-Drs. 17/7746) vorgelegt. Der Entwurf enthielt aus datenschutzrechtlicher Sicht Verbesserungen gegenüber den bisherigen Referentenentwürfen. Insbesondere die Einwilligungslösung fand bei einfachen Melderegisterauskünften für Zwecke der Werbung und des Adresshandels Berücksichtigung. Aber auch der Verzicht auf ein zentrales Bundesmelderegister fand die Zustimmung der Datenschutzbeauftragten des Bundes und der Länder.

Bedauerlich war, dass die weitere Stärkung der Rechte der Meldepflichtigen, die Abschaffung der Hotelmeldepflicht sowie die Forderung der Nichteinführung der Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters nicht im Regierungsentwurf berücksichtigt worden sind.

In seinem Gesetzesbeschluss vom 28. Juni 2012 hat der Deutsche Bundestag die im Regierungsentwurf enthaltenen Datenschutzbestimmungen wieder verworfen bzw. verschlechtert. So wurde die bisher vorgesehene Einwilligungslösung bei den einfachen Melderegisterauskünften für Zwecke der Werbung und des Adresshandels durch eine Widerspruchslösung ersetzt. Des Weiteren wurde das Widerspruchsrecht gegen die Erteilung einfacher Melderegisterauskünfte im Wege des automatisierten Abrufs über das Internet gestrichen und die einfache Melderegisterauskunft zu sonstigen gewerblichen Zwecken auf Zwecke der Werbung und des Adresshandels begrenzt. Das Widerspruchsrecht sollte dann nicht gelten, wenn eine Firma die Auskunft lediglich zur Korrektur vorhandener Datenbestände erhalten sollte. Damit wurde eine daten- und verbraucherschutzfreundliche Regelung abgelehnt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 22. August 2012 „Melderecht datenschutzkonform gestalten!“ (**Anlage 15**) und in einer gemeinsamen Stellungnahme den Bundesrat aufgefordert, dem Gesetz nicht zuzustimmen und auf die beträchtlichen datenschutzrechtlichen Defizite hingewiesen.

Mit Blick auf die ausstehenden Beratungen im Bundesrat hat der Landesbeauftragte die Gelegenheit genutzt, den Minister für Inneres und Sport des Landes Sachsen-Anhalt auf die datenschutzrechtlichen Mängel aufmerksam zu machen.

Im Vermittlungsausschuss haben sich Bund und Länder nach langen Verhandlungen beim geplanten Melderecht geeinigt. Der gefundene Kompromiss sieht nun wieder die Einwilligungslösung bei den einfachen Mel-

deregisterauskünften für Zwecke der Werbung und des Adresshandels vor. Von einer Widerspruchslösung wurde abgesehen (§ 44 Abs. 3 Nr. 2 Bundesmeldegesetz).

Das vom Bundestag mit Zustimmung des Bundesrates beschlossene Gesetz zur Fortentwicklung des Meldewesens vom 3. Mai 2013 (BGBl. I S. 1084) tritt mit Wirkung vom 1. Mai 2015 in Kraft.

Es bleibt nun abzuwarten, wann und wie der Aufbau und Betrieb eines zentralen Meldedatenbestandes auf Landesebene zur Sicherstellung eines jederzeit automatisierten Abrufs von Meldedaten durch öffentliche Stellen umgesetzt wird, der die bundesrechtlichen Anforderungen aus dem Bundesmeldegesetz erfüllt.

5.9.2 Meldedaten an Religionsgemeinschaften und GEZ

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich mit der Übermittlung von Daten von Meldebehörden an öffentlich-rechtliche Religionsgemeinschaften und die GEZ. Teilweise wurden die sensiblen Daten durch die Meldebehörden unverschlüsselt versandt.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung „Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten“ vom 8. November 2012 (**Anlage 17**) insbesondere gefordert, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren zu verwenden und dem Bundesministerium des Innern empfohlen, die Verwendung des Protokollstandards OSCI-Transport vorzuschreiben sowie die gesetzlichen Vorgaben umzusetzen.

Das Ministerium des Innern des Landes Sachsen-Anhalt hatte zwischenzeitlich den Landesbeauftragten darüber informiert, dass die rechtskonforme Verschlüsselung in der Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden in Sachsen-Anhalt umgesetzt wurde.

5.9.3 Veröffentlichung von Jubiläumsdaten

Im Rahmen einer Eingabe wurde dem Landesbeauftragten bekannt, dass das Geburtstagsjubiläum einer Petentin in der regionalen Zeitung veröffentlicht wurde, obwohl sie eine Auskunfts- und Übermittlungssperre beantragt hatte.

Grundsätzlich erfolgt durch das Einwohnermeldeamt die Übermittlung einer Liste der Geburtsjubilare an die regionale Zeitung monatlich am 15. für den darauffolgenden Monat. Der Antrag einer Auskunfts- bzw. Übermittlungssperre wurde am 17. des Monats gestellt und am 18. im Melderegister erfasst. In der Regel wird die regionale Zeitung unmittelbar über Änderungen, die sich aus einem Antrag auf Auskunfts- bzw. Übermittlungssper-

ren ergeben, informiert. In diesem speziellen Fall wurde es versäumt, die Änderung der regionalen Zeitung mitzuteilen.

Die Stadt hat sich bei der Petentin für ihr Fehlverhalten entschuldigt und ihre eigenen Mitarbeiterinnen und Mitarbeiter nochmals sensibilisiert, um künftig solchen Fehlern vorzubeugen.

5.9.4 Gruppenauskunft über Jubiläumsdaten an Kommunalparlamente

Eine Stadt bat den Landesbeauftragten um Klärung, ob eine Gruppenauskunft zum Zweck der Veröffentlichung von Alters- und Ehejubiläen möglich wäre, auch wenn dies weder im Meldegesetz des Landes Sachsen-Anhalt (MG LSA) noch im DSG LSA erwähnt wird. Des Weiteren war zu klären, ob eine Weitergabe der o. g. Daten an einen Kreistag zulässig sei.

Da die o. a. Angelegenheit nicht nur melderechtliche Aspekte berührt, sondern auch mit Blick auf die Ausführungen zur Praxis bei der Veröffentlichung von Altersjubiläen in den Amtsblättern der Stadt sowie des Landkreises eine Bewertung aus kommunalrechtlicher Sicht bedurfte, hatte der Landesbeauftragte das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt in das Verfahren einbezogen, um eine Abstimmung von kommunalrechtlichen und von datenschutzrechtlichen Fragestellungen zu ermöglichen.

Als Melderegisterauskünfte in besonderen Fällen lässt § 34 Abs. 2 MG LSA die Erteilung einer Gruppenauskunft über Alters- und Ehejubiläen an Presse und Rundfunk sowie Mitglieder parlamentarischer und kommunaler Vertretungskörperschaften zu, soweit die Betroffenen dieser Auskunftserteilung nicht widersprochen haben (§ 34 Abs. 4 MG LSA).

Soweit Presse und Rundfunk Gruppenauskünfte über Alters- und Ehejubiläen erhalten, werden diese zur entsprechenden Veröffentlichung im jeweiligen Medium erteilt, auch wenn dieser Verwendungszweck nicht ausdrücklich normiert ist.

Zu den parlamentarischen und kommunalen Vertretungskörperschaften, deren Mitglieder ebenfalls eine Gruppenauskunft über Alters- und Ehejubiläen erhalten können, gehören auch die Gemeinderäte und Kreistage. Gesetzliche Mitglieder der Gemeinderäte sind nach § 36 Abs. 1 Satz 1 Gemeindeordnung für das Land Sachsen-Anhalt (GO LSA) die ehrenamtlichen Mitglieder (Gemeinderäte) und der Bürgermeister; die Kreistage bestehen nach § 25 Abs. 1 Landkreisordnung für das Land Sachsen-Anhalt (LKO LSA) aus den ehrenamtlichen Mitgliedern und dem Landrat. Die Regelung in § 34 Abs. 2 MG LSA, die es allen Mitgliedern parlamentarischer und kommunaler Körperschaften ermöglichen soll, Alters- und Ehejubilaren Glückwünsche auch im Namen des Gemeinderates oder Kreistags zu übermitteln, lässt somit auch die Erteilung einer Gruppenauskunft an den Bürgermeister bzw. Landrat als Mitglied des Gemeinderates bzw. Kreistages zu.

Unabhängig davon können der Bürgermeister bzw. die zuständigen Stellen der Gemeinden Daten aus dem Melderegister erhalten, sofern die Kenntnis der Daten zur Aufgabenerfüllung, z. B. zu Repräsentationszwecken, erforderlich ist. Dabei genügt es nicht, wenn die Bekanntgabe der Daten zur Aufgabenerfüllung nur dienlich oder nützlich ist, sie muss vielmehr hierfür unbedingt notwendig sein. In diesen Fällen handelt es sich nicht um eine Gruppenauskunft nach § 34 Abs. 2 MG LSA, sondern um eine Datenweitergabe innerhalb der Verwaltung nach § 29 Abs. 5 MG LSA, bei der zum Zwecke der Sensibilisierung des Datenempfängers auch evtl. im Melderegister eingetragene Übermittlungssperren mitzuteilen sind.

Die Gratulation oder Ehrung anlässlich eines besonderen Jubiläums durch die Gemeinde entspricht häufig einer langen Tradition und wird vielfach auch von den Alters- und Ehejubilaren erwartet. Wie die Gemeinde ihre Alters- und Ehejubilare ehrt (Besuch des Bürgermeisters oder eines anderen Vertreters der Gemeinde, Blumen- oder Kartengruß etc.), dürfte dabei unter Berücksichtigung der ortsüblichen Gegebenheiten zu regeln sein.

Die Datenübermittlung an die Landkreisverwaltung für Zwecke der Ehrung bei Alters- und Ehejubiläen richtet sich dagegen nach § 5 Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden in Sachsen-Anhalt. Danach dürfen dem Landkreis für Ehrungen aus Anlass des 50., 60., 65., 70. und 75. Hochzeitstages sowie zur Vollendung des 100. und eines jeden weiteren Lebensjahres regelmäßig bestimmte Daten der Betroffenen übermittelt werden.

Auch hier ist die Tatsache, dass eine Übermittlungssperre nach § 34 Abs. 4 in Verbindung mit Abs. 2 MG LSA vorliegt, mitzuteilen.

Aus kommunalrechtlicher Sicht dürfte der örtlichen und überörtlichen Bekanntmachung von Alters- und Ehejubiläen in Amtsblättern der Kommunen keine kommunalrechtliche Norm entgegenstehen. Als Amtsblatt bezeichnet man ein behördliches Mitteilungsblatt für amtliche Bekanntmachungen, welche die Allgemeinheit betreffen und dazu dienen, einen Sachverhalt öffentlich bekannt zu geben. Teilweise beziehen sich die Bekanntmachungen auch auf den internen Dienstbetrieb. Neben den öffentlichen Bekanntmachungen der Gemeinde können im Amtsblatt auch weitere nichtamtliche Informationen für die Bürger aufgenommen werden. Als Beiträge im nichtamtlichen Teil des Amtsblattes können Berichte, Meinungsäußerungen, Nachrichten oder Hinweise sowohl der Gemeinde als auch Dritter zu örtlichen Ereignissen wie kommunalpolitischen Fragen und Themen in Betracht kommen. Dem Amtsblatt kommt insoweit in seinem nichtamtlichen Teil die Funktion eines Informationsinstrumentes der Gemeinde zu. Hat sich die Gemeinde entschieden, das Amtsblatt auch zur Veröffentlichung nichtamtlicher Informationen zugänglich zu machen, steht es im Ermessen der Gemeinde, welche Beiträge sie unter Berücksichtigung der melderechtlichen Vorschriften (§ 34 MG LSA) im nichtamtlichen Teil abdrucken lässt. Die presserechtliche Verantwortung für das Amtsblatt liegt bei der Gemeinde bzw. der herausgebenden Körperschaft.

Mit Blick darauf, dass Auskünfte über Alters- und Ehejubiläen unter Beachtung des Widerspruchsrechts der Betroffenen nach § 34 Abs. 4 MG LSA auch an Presse und Rundfunk erteilt werden dürfen, wird die (parallele) Veröffentlichung auch in Amtsblättern mit den entsprechenden Glückwünschen des Herausgebers im Namen der Gemeinde bzw. des Landkreises zumindest immer dann für unproblematisch gehalten, wenn auch hier eine bestehende Auskunftssperre beachtet wird.

5.10 Benutzung der Personenstandsregister

Die Personenstandsregister werden elektronisch geführt (§ 3 Abs. 2 Satz 1 Personenstandsgesetz (PStG)). In einer Übergangszeit, die am 31. Dezember 2013 endet, können Standesämter, die am 1. Januar 2009 noch nicht über eine Ausstattung zur elektronischen Führung der Personenstandsregister verfügten, Personenstandsfälle in einem Papierregister beurkunden (§ 75 Satz 1 PStG); vgl. IX. Tätigkeitsbericht, Nr. 7.6.

Der Landesbeauftragte erhielt eine Eingabe zur Frage, ob Vollauskünfte aus dem Personenstandsregister und den Sammelakten zulässig seien. Im Ergebnis der Prüfung wurde festgestellt, dass der Petentin ein erweiterter Zugang zu den Sammelakten der verstorbenen Eltern möglich ist.

Grundlage für die Beurteilung eines Auskunftsrechtes und die Einsichtnahme in Personenstandsurkunden und in Sammelakten bildet § 62 i. V. m. § 61 PStG. Danach hat die Petentin, was das Eheregister und die Sammelakten ihrer Eltern betrifft, ein uneingeschränktes Benutzungsrecht.

Dieses wird nur dadurch eingeschränkt, dass in der Sammelakte auch Angaben zu anderen Personen vorhanden sein könnten (z. B. in Scheidungsurteilen oder anderen Dokumenten), die wiederum ein eigenes datenschutzrechtliches Interesse an ihren Daten haben. Die Benutzung dieser Daten richten sich entweder nach § 62 Abs. 3 PStG (Tod des zuletzt Beteiligten vor 30 Jahren) oder nach allgemeinen datenschutzrechtlichen Bestimmungen, je nachdem ob die Unterlagen in einer Sammelakte aufzubewahren sind, oder in einer sonstigen Akte. Die personenstandsrechtliche Benutzung der Sammelakte wäre beispielsweise dann zu versagen bzw. einzuschränken, wenn das Standesamt nur mit unverhältnismäßig hohem Aufwand feststellen kann, ob die sonstigen Beteiligten, die in der Sammelakte erscheinen, bereits seit 30 Jahren tot sind.

Die vorstehende Rechtsanwendung wurde mit dem Standesamt der Stadt einvernehmlich abgestimmt. Im Ergebnis könnte jedoch eine uneingeschränkte Benutzung am Nichtvorhandensein der Sammelakte der ersten Ehe, an datenschutzrechtlichen Belangen Dritter sowie am unverhältnismäßigen Rechercheaufwand des Standesamtes scheitern.

5.11 Änderung Ausländerzentralregistergesetz

Im Oktober 2011 wurde der Landesbeauftragte durch ein Schreiben eines anderen Landesbeauftragten auf einen neuen Referentenentwurf zur Än-

derung des Ausländerzentralregistergesetzes (AZRG) (siehe auch X. Tätigkeitsbericht, Nr. 5.2) aufmerksam gemacht.

Mit diesem Gesetzentwurf sollte der Umfang der von Unionsbürgern gespeicherten Daten begrenzt werden. So wurde z. B. auf die Speicherung eines Lichtbildes im Ausländerzentralregister verzichtet. Des Weiteren wurde klargestellt, dass eine Speicherung der Daten von Unionsbürgern nur zu ausländer- und asylrechtlichen Zwecken erlaubt ist und die Weitergabe der Daten nur an Behörden, die mit diesen Aufgaben betraut sind, erlaubt ist.

Auch an diesem Gesetzentwurf gab es Kritikpunkte, auf die der Landesbeauftragte das Ministerium für Inneres und Sport hinwies. So liegt der Umfang der zu speichernden Daten für Unionsbürger noch immer über den Vorgaben, die nach der EuGH-Entscheidung vom 16. Dezember 2008 (NVwZ 2009, 379) zulässig wären. Des Weiteren kritisierte der Landesbeauftragte die Regelungen zur Übermittlung von Daten zu Unionsbürgern und zur Gruppenauskunft, da auch hier nicht ausgeschlossen werden kann, dass Daten von Unionsbürgern mitübermittelt werden.

In der Folgezeit wurde das Gesetz von Bundestag und Bundesrat verabschiedet (BGBl. I 2012 S. 2745) und trat zum größten Teil zum 1. September 2013 in Kraft. Die Änderungen des AZRG bedingen ebenfalls eine Anpassung der AZRG-Durchführungsverordnung, welche zeitnah umgesetzt werden soll, um die geänderten gesetzlichen Vorgaben zu erfüllen.

5.12 Sicherheitsakten

In seinem X. Tätigkeitsbericht (Nr. 26.4) hat der Landesbeauftragte bereits das Thema Sicherheitsüberprüfungen aus dem Blickwinkel des Widerspruchsrechtes der Betroffenen gegen die Einsichtnahme in Unterlagen der Sicherheitsüberprüfung beleuchtet. Im Berichtszeitraum des XI. Tätigkeitsberichtes hat der Landesbeauftragte dann zwei oberste Landesbehörden – Ministerien – auf die Einhaltung der Vorschriften zum Umgang mit Sicherheitsakten hin kontrolliert. Die Ergebnisse können als durchwachsen beschrieben werden.

Zu Beginn soll der etwas sperrige Begriff der „Sicherheitsakte“ kurz erläutert werden. Personen, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, sind vorher einer Sicherheitsüberprüfung zu unterziehen. Eine sicherheitsempfindliche Tätigkeit übt u. a. aus, wer Zugang zu Verschlusssachen hat, die als VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM eingestuft sind. Darüber hinaus übt eine sicherheitsempfindliche Tätigkeit aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung beschäftigt ist (§ 2 Abs. 1 SÜG-LSA).

Die Art der Sicherheitsüberprüfung hängt dabei davon ab, welche Berechtigung der Person nach Abschluss erteilt werden soll. Es gibt drei Stufen der Sicherheitsüberprüfung – Ü1, Ü2 und Ü3. Ü1 wird überprüft, wer ermächtigt werden soll, Zugang zu Unterlagen bis zum Verschlusssachen-

grad VS-VERTRAULICH zu haben. Ü2 wird überprüft, wer ermächtigt werden soll, Zugang zu Unterlagen bis zum Verschlusssachengrad GEHEIM zu haben und Ü3 wird überprüft, wer als STRENG GEHEIM eingestufte Unterlagen bearbeiten soll. Dabei gilt: Je höher die Ermächtigung, umso intensiver die Sicherheitsüberprüfung. Bei einer Ü1 wird nur der Betroffene selbst überprüft. Bei einer Ü2 werden Ehegatten, Lebenspartner oder Lebensgefährten der Betroffenen in die Überprüfung einbezogen. Und bei einer Ü3 werden im Rahmen der Überprüfung Referenz- und Auskunftspersonen über den Betroffenen befragt. Der datenschutzrechtliche Eingriff dabei wird für den Betroffenen immer intensiver, je höher seine Ermächtigung am Ende ausfallen soll.

Für die Sicherheitsüberprüfung werden zwei Akten zur Person des Betroffenen geführt, die Sicherheitsakte und die Sicherheitsüberprüfungsakte (§ 20 SÜG-LSA). Die Sicherheitsakte führt die zuständige Stelle, bei der der Betroffene die sicherheitsempfindliche Tätigkeit aufnehmen soll. In ihr sind Informationen über die persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse des Betroffenen aufzunehmen. Darüber hinaus wird eine Sicherheitsüberprüfungsakte bei der mitwirkenden Behörde – in Sachsen-Anhalt der Verfassungsschutzbehörde – geführt.

Ein Recht des Betroffenen auf Auskunft und Akteneinsicht in diese Akten wird im § 25 SÜG-LSA geregelt. Die Auskunft und Akteneinsicht ist allerdings nicht umfassend und für alle Daten vorgesehen und kann unter bestimmten Voraussetzungen sogar gänzlich verweigert werden. Deshalb ist es in diesem Bereich umso wichtiger, dass der Landesbeauftragte die Einhaltung der gesetzlichen Vorgaben überprüft.

Bei einem Ministerium konnte der Landesbeauftragte im Ergebnis feststellen, dass datenschutzrechtlichen Regelungen im Zusammenhang mit dem Führen von Sicherheitsakten bezogen auf die Aufbewahrung im erforderlichen Umfang Rechnung getragen wurde. Hinsichtlich der datenschutzrechtlich relevanten materiellen Anforderungen nach dem SÜG-LSA wurde der Eindruck gewonnen, dass Überprüfungsvorgänge neueren Datums nur ganz vereinzelt mit datenschutzrechtlichen Regelungen nicht zu vereinbaren sind. Vorgänge älteren Datums wiesen allerdings eine tendenziell leicht höhere Quote auf. Vor dem Hintergrund der positiven Entwicklung konnte der Landesbeauftragte davon ausgehen, dass die aufgezeigten Mängel in eigener Verantwortung zeitnah beseitigt werden würden.

Dem zweiten kontrollierten Ministerium, dem Justizministerium, konnte der Landesbeauftragte lediglich hinsichtlich der Aufbewahrung der Sicherheitsakten ein positives Zeugnis ausstellen. Zu den materiellen Anforderungen nach dem SÜG-LSA musste allerdings festgestellt werden, dass die Überprüfungsvorgänge überwiegend nicht mit den datenschutzrechtlichen Anforderungen, die sich aus dem SÜG-LSA ergeben, zu vereinbaren waren. So wurden z. B. regelmäßig Überprüfungen der höchsten Sicherheitsstufe Ü3 durchgeführt, die Betroffenen allerdings nur zum Umgang mit Verschlusssachen bis zum Geheimhaltungsgrad GEHEIM ermächtigt. Für eine solche Ermächtigung hätte aber eine Überprüfung Ü2 ausgereicht. Neben der Beseitigung der festgestellten Mängel hat der Landes-

beauftragte eine eher grundlegende Auseinandersetzung mit der Frage nach der angemessenen Verwaltung von Sicherheitsakten angeregt und auf deren besondere Bedeutung und Obliegenheitspflicht gegenüber den Betroffenen verwiesen. Der Landesbeauftragte wird die Umsetzung seiner Empfehlungen und die Maßnahmen zur Sicherstellung datenschutzrechtlicher Belange begleiten; allerdings lag die Stellungnahme des Ressorts auch nach über sechs Monaten noch nicht vor.

Die Ergebnisse der Kontrollen zeigen, dass es im Interesse der Betroffenen erforderlich ist, die Einhaltung gesetzlicher Vorgaben im Umgang mit Sicherheitsakten zu prüfen. Der Landesbeauftragte wird derartige Kontrollen auch in Zukunft durchführen.

6 Landtag

6.1 Prüfung des Landesrechnungshofs bei Landtagsabgeordneten

Im X. Tätigkeitsbericht (Nr. 17.1) hat der Landesbeauftragte zu Prüfungen der Landtagsverwaltung durch den Landesrechnungshof berichtet. Infolge von Presseberichten über Internetrecherchen des Landesrechnungshofs zur Verwendung der Entschädigung durch die Abgeordneten hat der Landesbeauftragte die Angelegenheit im Sommer 2011 noch einmal aufgenommen. Dies eröffnete die Gelegenheit, den Vorgang nochmals ausführlich mit dem Landesrechnungshof und auch dem Landtagspräsidenten zu erörtern.

Grundsätzlich stehen dem Landesrechungshof umfängliche Prüfungsrechte zu. Die Grundlage bilden die Verfassung des Landes Sachsen-Anhalt (Art. 97, 98) und die speziellen Vorschriften der Landeshaushaltsordnung (§§ 88, 91, 94, 95 LHO). Dies schließt, wie im X. Tätigkeitsbericht dargestellt, die Befugnis ein, auch bei Dritten, die selbst nicht Adressat der Prüfung sind, als Empfänger von Aufwendungsersatz zu recherchieren. Die Erhebung von im Internet verfügbaren Kommunikationsinhalten, die sich an jedermann oder zumindest einen nicht weiter abgegrenzten Personenkreis richten, durch eine staatliche Stelle stellt zudem nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, Urteil vom 27. Februar 2008, NJW 2008, 822) nicht notwendig einen Eingriff in das allgemeine Persönlichkeitsrecht dar (vgl. auch BVerwG, Urteil vom 21. Juli 2010, NVwZ 2011, 161).

Der Landesbeauftragte konnte in den Erörterungen darauf hinweisen, dass unbeschadet dessen die Rahmenbedingungen zu berücksichtigen sind. So stehen die Befugnisse unter dem verfassungsrechtlichen Vorbehalt der Verhältnismäßigkeit, insbesondere im Hinblick auf das Ausmaß der Recherchen. Der Abgeordnetenstatus bzw. die Unabhängigkeit der Mandatsausübung ist zu beachten. Zudem kann ein Eingriff in das Persönlichkeitsrecht nach der o. g. Rechtsprechung dennoch gegeben sein, wenn Informationen gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet werden. Auch sind Stigmatisierungen der Beteiligten zu vermeiden, insbesondere soweit sie wie hier nicht selbst Adressat der Prüfung sind. Ein Gefühl des Überwachtwerdens

konnte durch nicht mitgeteilte Recherchen und generelle Vorwürfe eines Missbrauchs der Wahlkreisbüropauschale für Parteizwecke entstehen, auch wenn sie „nur“ die Sozialsphäre der Abgeordneten in ihrem Mandatsumfeld betrafen. Der Landesbeauftragte sah eine solche Gefährdungslage, es gab aber keine Beschwerde eines Abgeordneten. Dem Landesrechnungshof wurde empfohlen, dem Transparenzgebot stärker Rechnung zu tragen. Dieser argumentierte dagegen, dass eine besondere Gefahrenlage nicht entstanden sei, auch weil nur Feststellungen getroffen wurden, bei denen eine Überschreitung der Grenze erlaubter Wahlkreisarbeit lediglich zu vermuten sei.

Die Dokumentation zu den Internetrecherchen wurde, da nicht (mehr) erforderlich, vernichtet.

6.2 Stellungnahmen in Petitionsverfahren

Bereits im Jahr 2007 hat der Landesbeauftragte die Praxis hinterfragt, bei Petitionen von Gefangenen dem Petitionsausschuss neben einer Stellungnahme des Ministeriums der Justiz auch eine von der jeweiligen Justizvollzugsanstalt entworfene Kurzcharakteristik des Gefangenen beizufügen.

Das Ministerium der Justiz teilte dem Petitionsausschuss Anfang 2008 mit, dass diese Charakterisierung künftig – soweit erforderlich – in Zitatform erfolgen solle. Das hätte den Vorteil, dass die Stellungnahme des Ministeriums auch weiterhin umfassend und vollständig sein würden, jedoch Daten Dritter, wie z. B. von Eltern und Geschwistern, nicht unter Namensnennung übermittelt werden müssten. Des Weiteren räumte das Ministerium ein, dass die Kurzcharakteristik zwar die Person des Petenten zu beschreiben vermag, für die Beurteilung des eigentlichen Anliegens aber in aller Regel nicht erforderlich sei. Der Petitionsausschuss zeigte sich dieser Auffassung gegenüber aufgeschlossen.

Mitte 2012 befasste sich der Ausschuss für Petitionen erneut mit der Frage, ob bei Petitionen aus dem Bereich der Justizvollzugsanstalten der Stellungnahme des Ministeriums die Genese des Gefangenen beigefügt bzw. als Vorbemerkung zur Stellungnahme aufgenommen werden solle. Gemeint waren hierbei vermutlich zusätzliche Informationen zur Person des Gefangenen und seine Entwicklung, die über die reine Sachinformation zum Beschwerdevorgang hinausgehen. Der Landesbeauftragte hat sich an den Vorsitzenden des Petitionsausschusses gewandt und darauf hingewiesen, dass die Kurzcharakteristik eines Gefangenen in aller Regel für die Beantwortung der Petition nicht erforderlich sei. Bei Bedarf bleibe es den Mitgliedern des Petitionsausschusses unbenommen, Nachfragen zu stellen. Der Landesbeauftragte unterstützt weitergehende Überlegungen des Petitionsausschusses, auf die Übermittlung von nicht erforderlichen, für das unmittelbare Verständnis des Beschwerdevorganges entbehrlichen Informationen generell zu verzichten. Eine solche Vorgehensweise würde eine grundrechtskonforme Berichterstattung sicherstellen (vgl. II. Tätigkeitsbericht, Nr. 16.2, und IV. Tätigkeitsbericht, Nr. 16).

Im Rahmen der Prüfung einer Eingabe eines Gefangenen der JVA Burg wurde dem Landesbeauftragten eine Stellungnahme des Ministeriums für Justiz und Gleichstellung an den Petitionsausschuss bekannt. Gegenstand war die Fehlleitung von Schriftstücken anderer Gefangener an den Petenten. Hierfür hat er die JVA Burg verantwortlich gemacht. Mit seinem Anliegen hat sich der Gefangene sowohl an den Petitionsausschuss des Landtages als auch an den Landesbeauftragten gewandt. Aus der Stellungnahme des Ministeriums für Justiz und Gleichstellung war ersichtlich, dass nicht die JVA, sondern das OLG Naumburg für das Postversehen verantwortlich war. Neben dieser kurzen Information wurde ergänzend eine ganze Reihe von personenbezogenen Daten dem Petitionsausschuss mitgeteilt. Dies reichte vom Geburtsdatum und Geburtsort über die Mitteilung der Gesamtfreiheitsstrafe, die Urteilsgründe, den Zwei-Drittel-Strafpunkt bis zum Strafzeitende. Darüber hinaus wurden Wertungen, wie der Petent sei umfangreich einschlägig vorbestraft und hafterfahren, mitgeteilt. Auch die Einträge aus dem Bundeszentralregister wurden zitiert. Diese Angaben machten knapp die Hälfte der Stellungnahme des Ministeriums aus.

Es war für den Landesbeauftragten nicht erkennbar, warum die Bekanntgabe dieser personenbezogenen Daten erforderlich sind, wenn ein Gefangener sich über ein vermeintliches Organisationsversagen der Anstalt beschwert. Aus diesem Grunde wurde das Ministerium für Justiz und Gleichstellung gebeten, zukünftig nur personenbezogene Daten von Gefangenen in Petitionen zu verwenden, soweit diese für das Verständnis der Petition im Einzelfall erforderlich sind.

Im Rahmen einer weiteren Petition wurde die Darstellung von sensiblen bzw. vertraulichen Inhalten, die u. a. auch Dritte betreffen können, problematisiert. Das Ministerium für Justiz und Gleichstellung hat in diesem Zusammenhang darauf hingewiesen, dass in Einzelfällen die Stellungnahmen der Landesregierung gegenüber dem Landtag auch Informationen enthalten können, die nicht für Außenstehende bestimmt sind. Da der Petitionsausschuss eine unbeabsichtigte Weitergabe solcher Informationen unbedingt vermeiden möchte, hat das Ministerium zugesagt, darauf hinzuwirken, dass in den Stellungnahmen des Justizvollzuges zu einzelnen Petitionen künftig die Informationen, die nur für den Ausschuss und nicht für Petenten oder Dritte bestimmt sind, besonders kenntlich gemacht werden.

7 Rechtspflege und Strafvollzug

7.1 Quellen-Telekommunikationsüberwachung

In seinem X. Tätigkeitsbericht hat der Landesbeauftragte unter Nr. 20.2 über die Quellen-Telekommunikationsüberwachung berichtet. Im Ergebnis seiner Anfragen an die zuständigen Ministerien konnte der Landesbeauftragte Anfang 2012 feststellen, dass Maßnahmen der Quellen-Telekommunikationsüberwachung durch Behörden in Sachsen-Anhalt

nicht veranlasst wurden. Bis dahin fehlte es für Sachsen-Anhalt auch an den erforderlichen Rechtsgrundlagen.

Mit der Novelle des SOG LSA 2013 wurde dann eine Rechtsgrundlage für die präventive Quellen-Telekommunikationsüberwachung durch die Polizei des Landes Sachsen-Anhalt geschaffen. Auf den Beitrag zur Änderung des SOG LSA unter Nr. 5.1 wird verwiesen.

Telekommunikationsüberwachungsmaßnahmen im Bereich des Verfassungsschutzes richten sich nach dem G 10-Gesetz (vgl. Nr. 8.4).

Über die Möglichkeiten, rechtmäßig eine Quellen-Telekommunikationsüberwachung im repressiven Bereich durchzuführen, die den Anforderungen des Bundesverfassungsgerichtes entspricht, gehen die Auffassungen durchaus auseinander. Im Dezember 2012 äußerte sich der Generalbundesanwalt dahingehend, dass eine Begrenzung der Maßnahme, wie sie das Bundesverfassungsgericht fordere, derzeit technisch nicht hinreichend gewährleistet werden könne. Das federführende Bundesministerium des Innern hingegen prüfe bestehende gesetzliche Regelungen der StPO auf deren Tragfähigkeit für Quellen-Telekommunikationsüberwachungsmaßnahmen.

Der Landesbeauftragte hält diesbezüglich an der durch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2011 vertretenen Rechtsauffassung fest, wonach die StPO keine Regelung enthalte, die den Anforderungen des Bundesverfassungsgerichtes an Quellen-Telekommunikationsüberwachungsmaßnahmen gerecht werde. Die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen müssen gesetzlich verankert sein (vgl. X. Tätigkeitsbericht, Nr. 20.2).

Der Aufforderung der Datenschutzbeauftragten des Bundes und der Länder, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären, ist der Gesetzgeber bisher nicht nachgekommen.

7.2 Vorratsdatenspeicherung

In seinem X. Tätigkeitsbericht (Nr. 25.1) berichtete der Landesbeauftragte darüber, dass das Bundesverfassungsgericht mit Urteil vom 2. März 2010 die Vorratsdatenspeicherung in der bisherigen Umsetzung für verfassungswidrig erklärt hatte, da die entsprechenden Regelungen des TKG und der StPO mit Art. 10 Abs. 1 GG (Fernmeldegeheimnis) nicht vereinbar sind.

Zwar ist laut Bundesverfassungsgericht eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein verfassungswidrig, es fehlt jedoch an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hin-

reichende Datensicherheit noch eine hinreichende Begrenzung der Verwendungszwecke der Daten.

Die Daten dürften nur für „überragend wichtige Aufgaben des Rechtsgüterschutzes“ abgerufen werden, z. B. bei begründetem Verdacht einer schweren Straftat. Bei der präventiven Arbeit der Polizei müsse eine konkrete Gefahr für Leib, Leben oder Freiheit von Personen bestehen. Eine Verwendung der Daten durch die Geheimdienste sei deshalb in vielen Fällen ausgeschlossen, weil diese ja weit im Vorfeld von Straftaten tätig würden.

Inzwischen hat die EU-Kommission Deutschland vor dem Europäischen Gerichtshof verklagt, weil es die entsprechende Richtlinie nicht umgesetzt hat. Gegenüber anderen Staaten wie z. B. Schweden wurden bereits Bußgelder verhängt. Eine Neuregelung der Vorratsdatenspeicherung wäre unter den strengen Voraussetzungen des Bundesverfassungsgerichtsurteils möglich. Allerdings ist die Umsetzung in nationales Recht bislang durch die andauernde rechtspoltische Diskussion zwischen dem Bundesministerium der Justiz und dem Bundesministerium des Innern verhindert worden. Die Bundesjustizministerin hatte vorgeschlagen, Verkehrsdaten bei einem begründeten Verdacht „einzufrieren“, also nicht auf Vorrat, sondern anlassbezogen zu speichern (Quick-Freeze-Verfahren). Dagegen wird von den Vertretern der Sicherheitsbehörden immer wieder betont, dass die Vorratsdatenspeicherung zur Aufklärung von Straftaten gerade im Internet unverzichtbar wäre und dafür das vorgeschlagene Quick-Freeze-Verfahren nicht ausreichend sei.

Die anderen EU-Staaten haben die Mindestvorgaben der Richtlinie unterschiedlich umgesetzt. So werden die Daten in zehn Staaten, darunter Frankreich und Spanien, ein Jahr lang gespeichert, in Polen sogar zwei Jahre. Auch die Hürden für den Zugriff sind unterschiedlich ausgestaltet. In Tschechien und Rumänien wurden die nationalen Gesetze – wie in Deutschland – für verfassungswidrig erklärt. Inzwischen haben aber auch diese Staaten neue Gesetze erlassen, sodass Deutschland derzeit als einziges Land die Richtlinie nicht umgesetzt hat. Das hängt damit zusammen, dass beim Europäischen Gerichtshof durch Irland und Österreich eine grundrechtliche Prüfung angestrebt worden ist.

7.3 PPP-Projekt Justizvollzugsanstalt Burg – Entwicklung/Sachstand

In seinem X. Tätigkeitsbericht hat der Landesbeauftragte die im Zusammenhang mit dem PPP-Projekt Justizvollzugsanstalt Burg aus datenschutzrechtlicher Sicht vom Ministerium für Justiz und Gleichstellung bzw. der JVA Burg zu erledigenden Aufgaben klar umschrieben (vgl. Nrn. 24.1 und 24.2 des X. Tätigkeitsberichts). Hierzu gehörten im Wesentlichen

- Schaffung einer Rechtsgrundlage für die Auftragsdatenverarbeitung in einem zukünftigen Erwachsenenstrafvollzugsgesetz,
- Abschluss eines Generalvertrags über die Auftragsdatenverarbeitung mit dem privaten Dienstleister,

- Erlass eines Datenschutzkonzepts in Form einer Dienstanweisung für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den privaten Dienstleister und
- Umsetzung der Empfehlungen aus dem Prüfbericht zum Informations- und Kontrollbesuch der JVA Burg, insbes. Rückübertragung der Befugnis zur Durchsuchung bzw. Absuchung von Besuchern durch den privaten Dienstleister auf staatliche Bedienstete.

Die Landesregierung hat in ihrer Stellungnahme zum X. Tätigkeitsbericht der Rechtsauffassung des Landesbeauftragten in den o. g. Punkten nicht widersprochen und angekündigt, die enge Abstimmung mit ihm zu suchen.

Der Landesbeauftragte hat auch klargestellt, dass er – sollte es in den kritischen Punkten nicht zu einer zufriedenstellenden Lösung kommen – sich eine Beanstandung der von ihm festgestellten Verstöße und Mängel nach § 24 DSG LSA ausdrücklich vorbehalte.

Die o. g. öffentlichen Stellen haben seit dem Informations- und Kontrollbesuch in der JVA Burg im Oktober 2010 für die Erfüllung Ihrer Aufgaben mehr als zwei Jahre Zeit gehabt. Trotz umfangreicher Beratung durch den Landesbeauftragten und mehrerer Arbeitstreffen ist jedoch festzustellen, dass im Berichtszeitraum einzelne Punkte gar nicht bzw. nur teilweise abgearbeitet wurden.

Schaffung einer Rechtsgrundlage für die Auftragsdatenverarbeitung

Seit 2007 besteht im Zusammenhang mit der Ausarbeitung des Datenschutzkonzepts mit dem Justizministerium Einvernehmen darüber, dass es sich bei der Erhebung, Verarbeitung und Nutzung durch den privaten Dienstleister um Auftragsdatenverarbeitung handelt. Da im Strafvollzugsgesetz eine Rechtsgrundlage für die Auftragsdatenverarbeitung fehlt, der teilprivatisierte Betrieb der JVA Burg insofern rechtswidrig ist, hatte der Landesbeauftragte in seinem X. Tätigkeitsbericht so schnell wie möglich die Schaffung einer entsprechenden Rechtsgrundlage in einem zukünftigen Erwachsenenstrafvollzugsgesetz angemahnt.

Das Justizministerium hat dem Landesbeauftragten im Berichtszeitraum zwar einen Gesetzentwurf über den Vollzug der Freiheitsstrafe und zur Änderung von Vollzugsgesetzen des Landes Sachsen-Anhalt zur Stellungnahme übersandt, der Regelungen zur Auftragsdatenverarbeitung, zur Videoüberwachung in Justizvollzugsanstalten und zur getrennten Führung von Gefangenenpersonal-, Gesundheits- und Therapieakten enthielt und damit auf Kritikpunkte aus dem Tätigkeitsbericht einging. Die Regelungen über die Auftragsdatenverarbeitung waren jedoch nicht ausgereift, da das DSG LSA u. a. nicht direkt, sondern analog zur Anwendung kommen sollte. Nicht nachvollziehbar war zudem, dass das zur Beseitigung des zuvor geschilderten rechtswidrigen Zustands benötigte Strafvollzugsgesetz erst im Jahr 2016 in Kraft treten sollte.

Seit der Stellungnahme des Landesbeauftragten zu diesem Gesetzesentwurf ist ein gewisser Stillstand zu verzeichnen. Dies dürfte im Wesentli-

chen auch darauf beruhen, dass das Ministerium für Justiz und Gleichstellung im Gesetzgebungsverfahren zum Sicherungsverwahrungsvollzugsgesetz des Landes Sachsen-Anhalt versuchte, die Auftragsdatenverarbeitung durch den privaten Dienstleister in der JVA Burg in eine Funktionsübertragung umzudeuten und hierfür eine weniger strenge Regelung zu schaffen (vgl. hierzu Nr. 7.4). Der Landesgesetzgeber hat sich dieser Auffassung, die dann wahrscheinlich auch auf den Strafvollzug übertragen worden wäre, nicht angeschlossen.

Auf einem Arbeitstreffen im Juni 2013 hat der Staatssekretär des Justizministeriums angekündigt, dass sich das Kabinett der Landesregierung Ende des Jahres 2013 mit dem Entwurf eines völlig neu gestalteten Erwachsenenstrafvollzugsgesetzes befassen werde. Das Gesetz werde Regelungen über die Auftragsdatenverarbeitung enthalten und solle schon vor 2016 in Kraft treten. Festzuhalten bleibt, dass eine wesentliche Voraussetzung für die Verarbeitung personenbezogener Daten durch den privaten Dienstleister noch immer nicht erfüllt ist.

Abschluss eines Generalvertrages über die Auftragsdatenverarbeitung

Konsens bestand grundsätzlich auch darüber, dass von der verantwortlichen Stelle, also der JVA Burg, mit dem privaten Dienstleister ein Generalvertrag über die Auftragsdatenverarbeitung nach § 8 DSG LSA geschlossen werden sollte. Trotz umfangreicher Beratung und Hilfestellung des Landesbeauftragten hat das Justizministerium jedoch den von ihm seit langem avisierten Vertrag nicht vorlegen können.

Ein sachlicher Grund für dieses Versäumnis war nicht ohne Weiteres erkennbar, zumal der Vertreter des privaten Dienstleisters auf einem Arbeitstreffen mit dem Landesbeauftragten keine Einwände gegen den Abschluss eines entsprechenden Vertrages geltend gemacht hatte. Die mit dem privaten Partner geschlossenen Dienstleistungsverträge waren zwar auch Gegenstand einer Überprüfung durch das Ministerium, die u. a. zu einer Kündigung der Verträge über die Reinigung, Entsorgung und Ausstattung, der EDV-Systembetreuung sowie der Verpflegung geführt hat. Die gekündigten Dienstleistungsverträge laufen jedoch ohne jede Änderung bis zum 30. April 2014 weiter. Unabhängig davon muss der private Dienstleister, um seine Verpflichtungen zu erfüllen, personenbezogene Daten verarbeiten. Durch die Kündigung einzelner Verträge wird ein Generalvertrag über die Auftragsdatenverarbeitung also nicht hinfällig.

Das Justizministerium hat auf dem bereits erwähnten Arbeitstreffen mit dem Landesbeauftragten im Juni 2013 zugesagt, einen entsprechenden Vertrag auszuarbeiten. Es wurde festgestellt, dass der private Dienstleister neben dem Erwachsenenstrafvollzug auch bei der Untersuchungshaft und der Sicherungsverwahrung zum Einsatz kommt; vertragliche Regelungen sind auch hierfür erforderlich.

Datenschutzkonzept in Form einer Dienstanweisung

Vereinbarungsgemäß hätte das Justizministerium das Datenschutzkonzept für die Verarbeitung personenbezogener Daten im Strafvollzug in der JVA Burg in Form einer Dienstanweisung spätestens bis Ende des Jahres 2011 vorlegen sollen. Die Dienstanweisung sollte dabei aus einem allgemeinen datenschutzrechtlichen Teil, einem besonderen auf den Datenschutz im Einsatzbereich des privaten Dienstleisters zugeschnittenen Teil und einem technisch organisatorischen Teil hinsichtlich der Datensicherheit bestehen.

Obwohl der Landesbeauftragte dem Ministerium umfangreich beratend zur Seite stand, gelang es diesem nicht, bis Ende des Jahres 2011 eine den Anforderungen des Datenschutzes entsprechende Dienstanweisung vorzulegen. Da Vorschläge des Landesbeauftragten auch teilweise nicht beachtet wurden, lag ein erster prinzipiell geeigneter Entwurf einer Dienstanweisung erst Mitte 2012 vor, der im Ergebnis gleichwohl noch überarbeitungsbedürftig war. Es ist daher enttäuschend, dass die Dienstanweisung von der JVA Burg in Kenntnis der Mängel einseitig und ohne Abstimmung mit dem Landesbeauftragten zum 1. Januar 2013 in Kraft gesetzt wurde.

Die JVA Burg hat inzwischen zugesagt, die Dienstanweisung zu überarbeiten und die Mängel zu beseitigen. Zugleich soll für die Verarbeitung personenbezogener Daten im Bereich der Sicherungsverwahrung eine entsprechende Dienstanweisung erarbeitet werden. Überarbeitete Versionen wurden im Oktober 2013 übersandt.

Umsetzung der Empfehlungen aus dem Prüfbericht zum Informations- und Kontrollbesuch der JVA Burg

Ein Großteil der Empfehlungen aus dem Prüfbericht ist mittlerweile umgesetzt, z. B. werden Gefangenenpersonal- und Therapieakten getrennt geführt. Die Schreibkräfte des privaten Dienstleisters kommen nach Angaben des Justizministeriums bei sensiblen Schreiben nicht zum Einsatz. Eine Überwachung der Telefongespräche der Gefangenen wird nur noch angekündigt, wenn sie auch tatsächlich erfolgt.

Nicht umgesetzt wurde dagegen bisher die Empfehlung des Landesbeauftragten, dass die Ab- bzw. Durchsuchung von Besuchern wieder vom staatlichen Personal, anstelle des privaten Dienstleisters durchgeführt werden soll. Zur Erinnerung: Nach dem ursprünglichen PPP-Vertragswerk war es nicht vorgesehen, dass der private Dienstleister die Besucher der JVA ab- bzw. durchsucht, vielmehr sollte hier staatliches Personal eingesetzt werden. Erst durch eine nachträgliche Änderung des Vertragswerks wurde diese Aufgabe dem privaten Dienstleister übertragen. Der Landesbeauftragte hat darauf hingewiesen, dass nicht nur die vertraglich vorgesehene körperliche Durchsuchung, sondern auch die Absuchung von Besuchern mit Hilfe von Metalldetektoren durch den privaten Dienstleister als Verwaltungshelfer rechtswidrig ist, da nach h. M. Verwaltungshelfer nicht in Grundrechte Dritter eingreifen dürfen. Die vom Justizministerium vertre-

tene Auffassung, dass es sich bei der Absuchung von Besuchern um einen geringfügigen Eingriff handele, lässt sich mit der Rechtsprechung, die dem Ministerium vorliegt, nicht vereinbaren. Danach handelt es sich bei der Absuchung mit Metalldetektoren um eine Durchsuchung, die einen erheblichen Grundrechtseingriff darstellt. Nicht nachvollziehbar ist auch die Erklärung des Ministeriums, dass der Einsatz des privaten Dienstleisters nur unter Aufsicht und Leitung eines Justizvollzugsbeamten erfolgen dürfe, sodass immer eine Doppelbesetzung gegeben sei. In diesem Fall könnte der Beamte ohnehin die Ab- oder Durchsuchung sinnvollerweise gleich selbst durchführen.

Der Landesbeauftragte hat daher darauf verwiesen, dass genügend Zeit bestanden hat, den rechtswidrigen Zustand zu beseitigen. Er hat eine Beanstandung für den Fall angekündigt, dass die Ab- bzw. Durchsuchung durch den privaten Dienstleister nicht eingestellt und wieder staatlichem Personal übertragen wird.

Das Justizministerium hat eine erneute Prüfung des Vorgangs zugesagt.

Fazit:

Es ist enttäuschend, dass das Justizministerium trotz der weit über den üblichen Rahmen hinausgehenden Beratung und Hilfestellung durch den Landesbeauftragten nicht in der Lage war, im Berichtszeitraum den Vorgang abzuschließen. Immerhin weiß das Ministerium schon seit dem Jahr 2007 (vgl. VIII. Tätigkeitsbericht, Nr. 22.1), dass Handlungsbedarf besteht. Der Landesbeauftragte erwartet insbesondere von den beteiligten öffentlichen Stellen, dass die aufgezeigten Probleme nunmehr kurzfristig angepackt und gelöst werden.

7.4 Sicherungsverwahrung

Das Bundesverfassungsgericht hat in seinem Urteil vom 4. Mai 2011 (NJW 2011, 1931) die Vorschriften des Strafgesetzbuches über die Unterbringung in der Sicherungsverwahrung für nicht mit dem Grundgesetz vereinbar und unter näher ausgeführten Maßgaben für längstens bis zum 31. Mai 2013 anwendbar erklärt. Es hat in diesem Zusammenhang den Gesetzgebern in Bund und Ländern aufgegeben, ein freiheitsorientiertes und therapiegerichtetes Gesamtkonzept der Sicherungsverwahrung zu entwickeln, das dem verfassungsrechtlichen „Abstandsgebot“ Rechnung trägt, demzufolge sich der Vollzug der Unterbringung in der Sicherungsverwahrung vom Vollzug der Strafhaft deutlich zu unterscheiden hat.

Mit dem Gesetz zur bundesrechtlichen Umsetzung des Abstandsgebots im Recht der Sicherungsverwahrung vom 5. Dezember 2012 ist zunächst der Bundesgesetzgeber tätig geworden und hat die strafrechtlichen Regelungen der Sicherungsverwahrung reformiert (BGBl. I 2012 S. 2425).

Sachsen-Anhalt hat der Rechtsprechung im Wesentlichen durch den Erlass eines Sicherungsverwahrungsvollzugsgesetzes (SVVollzG LSA, Gesetz vom 13. Mai 2013, GVBl. LSA S. 206) Rechnung getragen. Unter da-

tenschutzrechtlichen Gesichtspunkten weist das neue Gesetz Licht und Schatten auf:

So hat der Landesgesetzgeber, um ein Beispiel für Schatten zu nennen, weitgehend die datenschutzrechtlichen Regelungen aus dem Strafvollzugsgesetz des Bundes in das SVVollzG LSA übernommen und neue Vorschriften zum Datenschutz nur geschaffen, soweit er dies für erforderlich hielt. Der Landesbeauftragte hat dies im Gesetzgebungsverfahren kritisiert, da ein Sicherungsuntergebrachter nicht ohne Weiteres mit einem Strafgefangenen verglichen werden kann. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt die Unterbringung für ihn nämlich ein Sonderopfer dar, weshalb er weniger tiefgehende Eingriffe zu dulden hat. Das Abstandsgebot ist daher auch datenschutzrechtlich zu berücksichtigen. Dies ist durch die prinzipielle Gleichbehandlung von Strafgefangenen und Sicherungsuntergebrachten aber nicht geschehen. Hinzu kommt, dass die übernommenen aus dem Jahre 1976 stammenden Regelungen des Strafvollzugsgesetzes des Bundes datenschutzrechtlich reformbedürftig sind.

Als Beispiel für Licht ist mit Blick auf den Einsatz eines privaten Dienstleisters in der Sicherungsverwahrung die Schaffung einer gesetzlichen Grundlage für die Auftragsdatenverarbeitung zu erwähnen. Der Gesetzesbegründung lässt sich entnehmen, dass der Vollzug der Sicherungsverwahrung in der JVA Burg erfolgen soll. Dabei soll – wie im Strafvollzug – in ausgewählten Bereichen auf Dienste eines privaten Partners zurückgegriffen werden, der personenbezogene Daten nur weisungsgebunden ohne eigene Entscheidungsbefugnis erheben, nutzen und verarbeiten darf. In seinem X. Tätigkeitsbericht hatte der Landesbeauftragte bereits dargestellt, dass es sich bei dem Einsatz des privaten Dienstleisters in der JVA Burg regelmäßig um Auftragsdatenverarbeitung handelt, die einer gesetzlichen Regelung bedarf (vgl. Nrn. 24.1 und 24.2 des X. Tätigkeitsberichts). Hierüber bestand mit dem Ministerium für Justiz und Gleichstellung seit langem Konsens. Einigkeit wurde mit dem Ministerium auch darüber erzielt, dass in dem PPP-Vertragswerk Regelungen zur Auftragsdatenverarbeitung fehlen und insofern der Abschluss eines neuen Vertrags über die Auftragsdatenverarbeitung erforderlich ist. Umso überraschter war der Landesbeauftragte, dass das Justizministerium im Gesetzgebungsverfahren die Datenverarbeitung des privaten Dienstleisters ursprünglich nicht als Auftragsdatenverarbeitung, sondern als Funktionsübertragung, d. h. als Datenübermittlung beschreiben und hierfür eine weniger strenge Regelung schaffen wollte. Kennzeichnend für eine Funktionsübertragung ist u. a. jedoch, dass personenbezogene Daten weisungsfrei mit eigener Entscheidungsbefugnis erhoben, genutzt und verarbeitet werden. Dies ist beim Einsatz des privaten Dienstleisters in der JVA Burg für den Bereich der Sicherungsverwahrung allerdings gar nicht vorgesehen. Der Landesgesetzgeber ist dem Vorschlag des Ministeriums daher zu Recht nicht gefolgt (vgl. §§ 98, 117 SVVollzG LSA i. V. m. § 8 DSG LSA).

Auf einem Arbeitstreffen mit dem Staatssekretär des Justizministeriums, dem Leiter der JVA Burg und der Projektgesellschaft Justizvollzug Burg hat der Landesbeauftragte auf die in der Praxis zu beachtenden Rechts-

folgen hingewiesen. Nachdem das SVVollzG LSA in Kraft getreten ist und die Sicherungsverwahrung auch tatsächlich in der JVA Burg vollzogen wurde, bedurfte es für den Einsatz des privaten Dienstleisters eines Vertrages über die Auftragsdatenverarbeitung. Dieser lag zum Zeitpunkt des Inkrafttretens des Gesetzes noch nicht vor und werde, so das Ministerium, nachgereicht. Der Leiter der JVA Burg hat zudem angekündigt, nach dem Vorbild für den Strafvollzug werde auch für die Sicherungsverwahrung ein Datenschutzkonzept in Form einer Dienstanweisung für die Verarbeitung personenbezogener Daten durch den privaten Dienstleister erlassen (vgl. Nr. 7.3).

7.5 Elektronische Fußfessel

In seinem X. Tätigkeitsbericht hat der Landesbeauftragte die Rechtsgrundlagen und das Verfahren für den Einsatz der elektronischen Aufenthaltsüberwachung die umgangssprachlich auch als elektronische Fußfessel bezeichnet wird, dargestellt (vgl. Nr. 24.4 des X. Tätigkeitsberichts). Hessen und Bayern haben zunächst als Vorreiter für die übrigen Länder den gemeinsamen Betrieb und die Nutzung der elektronischen Fußfessel durch eine Verwaltungsvereinbarung auf den Weg gebracht und einen Staatsvertrag zur Einrichtung einer Gemeinsamen elektronischen Überwachungsstelle der Länder (GÜL) mit Sitz im hessischen Bad Vilbel geschlossen. Diese hat zum 1. Januar 2012 ihren Betrieb aufgenommen. Mittlerweile haben auch die übrigen Länder die Verwaltungsvereinbarung unterzeichnet und sind dem Staatsvertrag beigetreten, so auch Sachsen-Anhalt (vgl. das Gesetz zum Beitritt des Landes Sachsen-Anhalt zum Staatsvertrag vom 13. März 2012, GVBl. LSA S. 114).

Im Gesetzgebungsverfahren zum Beitritt zum Staatsvertrag wurden die vom Landesbeauftragten im X. Tätigkeitsbericht aufgeworfenen datenschutzrechtlichen Fragestellungen zum Anlegen der Fußfessel durch einen privaten Dienstleister und zur Rechtmäßigkeit des Lesezugriffs der Polizei der in Hessen anfallenden personenbezogenen Daten nur gestreift, zu wichtig war wohl die Einführung der Fußfessel an sich. Kritisch anzumerken ist allerdings, dass das Ministerium für Justiz und Gleichstellung von einer Anhörung des Landesbeauftragten sogar gänzlich absehen wollte, weil Belange Dritter angeblich nicht berührt seien. Da beim Einsatz der Fußfessel personenbezogene Daten des Probanden erhoben und auch an die sachsen-anhaltische Polizei übermittelt werden, wurde diese offensichtlich unzutreffende Auffassung – zumal auch die Berichterstattung zum X. Tätigkeitsbericht vorlag – vom Ausschuss für Recht, Verfassung und Gleichstellung nicht geteilt.

Ob sich die elektronische Fußfessel in der Praxis bewährt, muss sich noch zeigen. Umso bedauerlicher ist es, dass der vom Ministerium seit 2011 avisierte Runderlass zur Umsetzung der elektronischen Aufenthaltsüberwachung sich noch in der Bearbeitung befindet und bisher nicht realisiert werden konnte.

7.6 Funkzellenabfrage

Die Strafverfolgungsbehörden in Dresden haben anlässlich von Versammlungen und gegen diese gerichteter Demonstrationen im Februar 2011 Funkzellenabfragen durchgeführt. Bei dieser Maßnahme wurden mehrere hunderttausend Verkehrsdaten von Mobilfunkverbindungen illegal erhoben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich daraufhin mit einer Entschließung im Juli 2011 „Funkzellenabfrage muss eingeschränkt werden!“ (**Anlage 1**) für die restriktive Handhabung der Funkzellenabfrage eingesetzt.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis nach Art. 10 des Grundgesetzes. Sie richtet sich gegen alle Besitzer von Mobilfunkgeräten, die sich in einer bestimmten Funkzelle aufhalten. Die Telekommunikationsüberwachung wird hingegen nur gegen bestimmte einzelne Tatverdächtige angewandt. Bei einer Funkzellenabfrage werden Art und Umstände der Kommunikation von Personen erfasst, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat den Bundesgesetzgeber daher aufgefordert, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken und die Löschungsvorschrift zu präzisieren. Die derzeitige Regelung in § 100g StPO ist unzureichend, weil sie weder hinreichend bestimmt ist noch den technischen Gegebenheiten der Gegenwart entspricht.

Über diese inhaltlichen Fragen hinaus sah sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlasst, die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verhaltensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung zu betonen. Die Kontrollkompetenz war zuvor in nicht nachvollziehbarer Weise in Frage gestellt worden. Mit ihrer Entscheidung „Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!“ (**Anlage 2**) erklärte die Konferenz der Datenschutzbeauftragten, dass die Befugnis zur Kontrolle außer Frage steht.

7.7 Beinahetreffer bei DNA-Reihenuntersuchungen

Bei der DNA-Reihenuntersuchung werden in der Regel mittels einer DNA-Analyse die genetischen Fingerabdrücke der untersuchten Bevölkerungsgruppe festgestellt. Zur Ermittlung des Täters, dessen DNA-Spuren vorliegen, kann sie entweder freiwillig oder auch auf richterliche Anordnung durchgeführt werden. Gesetzliche Grundlage für die DNA-Reihenuntersuchung ist § 81h StPO.

Neben anderen datenschutzrechtlichen Fragestellungen tauchte im Rahmen der DNA-Reihenuntersuchung das Problem der sog. Beinahetreffer auf. Diese liegen vor, wenn sich bei einem Getesteten ein DNA-Identifizierungsmuster ergibt, das mit den Spuren am Tatort zwar nicht vollständig übereinstimmt, aber eine so hohe Übereinstimmung aufweist, dass dies auf eine Verwandtschaft zwischen dem Getesteten und dem Täter schließen lässt. Dies kann im Einzelfall dazu führen, dass ein Vater, der freiwillig an der DNA-Reihenuntersuchung teilgenommen hat, unfreiwillig dafür sorgt, dass ein naher Verwandter, der nicht an dem Massengentest teilgenommen hat, in die weiteren Ermittlungen einbezogen und damit überführt wird.

Der BGH hat mit Urteil vom 20. Dezember 2012 (NJW 2013, 1827) entschieden, dass die Verwertung der sog. Beinahetreffer unzulässig ist. Zur Begründung wurde ausgeführt, dass § 81h Abs. 1 StPO den Abgleich von DNA-Identifizierungsmustern nur erlaube, soweit dies zur Feststellung erforderlich sei, ob das Spurenmaterial von einem der Teilnehmer der Reihenuntersuchung stamme. Damit hat der BGH festgelegt, dass die Verwendung der Daten aus DNA-Reihenuntersuchungen unzulässig sind, soweit daraus ein Tatverdacht gegen Dritte hergeleitet wird.

Der BGH hat mit dieser Grundsatzentscheidung rechtliche Klarheit über die Bewertung von Beinahetreffern bei DNA-Reihenuntersuchungen geschaffen. Dies ist auch aus datenschutzrechtlicher Sicht zu begrüßen.

7.8 Schuldnerverzeichnis im Internet

Seit dem 1. Januar 2013 ist das Gemeinsame Vollstreckungsportal der Länder (www.vollstreckungsportal.de) verfügbar. Hier werden die bundesweiten Daten aus den Schuldnerverzeichnissen nach §§ 882b ff. ZPO zum kostenpflichtigen Abruf bereitgestellt.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung (BGBl. I S. 2258) wurden im Jahre 2009 die rechtlichen Voraussetzungen hierfür geschaffen, sodass der Inhalt der Schuldnerverzeichnisse nunmehr über eine zentrale länderübergreifende Abfrage im Internet eingesehen werden kann. Die Einzelheiten der Einsichtnahme sollten vom Bundesministerium der Justiz durch eine Rechtsverordnung geregelt werden. Mit dieser sollte auch eine datenschutzgerechte Umsetzung der Einsichtnahme in das elektronische Vollstreckungsportal sichergestellt werden.

Diesen Anforderungen wurden die ersten Überlegungen einer solchen Verordnung nicht gerecht. Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke. Diese sind bei der Anfrage darzulegen. Dennoch war vorgesehen, dass bereits nach Eingabe des Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die beide Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Land eingerichtet sind, erhielt die anfragende Person bei einer Vielzahl

von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Vor diesem Hintergrund fasste die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung (**Anlage 9**) mit dem Ziel, die Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Die Datenschutzbeauftragten hielten es für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe von weiteren Identifizierungsmerkmalen vorzusehen.

Das Bundesministerium der Justiz hat mittlerweile eine Schuldnerverzeichnisführungsverordnung (BGBl. I 2012 S. 1654) erlassen. Darin wird mindestens die Eingabe des Namens und Vornamens des Schuldners oder der Firma des Schuldners und des Sitzes des zuständigen zentralen Vollstreckungsgerichts oder des Wohnsitzes des Schuldners oder des Ortes, an dem der Schuldner seinen Sitz hat, gefordert. Bei mehreren Datensätzen muss der Nutzer zusätzlich auch das Geburtsdatum des Schuldners eingeben. Sollten danach wiederum mehrere Datensätze vorhanden sein, ist auch noch die Angabe des Geburtsortes des Schuldners erforderlich. Erst wenn nach dieser Filterung noch mehrere Datensätze vorhanden sind, sind diese zu übermitteln. Im Ergebnis stellt die erlassene Schuldnerverzeichnisführungsverordnung eine datenschutzrechtlich verbesserte Regelung dar. Es bleibt abzuwarten, wie sie sich in der Praxis bewähren wird.

7.9 Elektronische Akte in der Justiz

Die Nutzung des elektronischen Rechtsverkehrs mit den Gerichten ist in Deutschland weit hinter den Erwartungen zurückgeblieben. Während in der Wirtschaft der Geschäftsverkehr in vielen Bereichen inzwischen auf elektronischem Wege abgewickelt wird, findet die Kernkommunikation mit der Justiz noch fast ausschließlich auf Papier statt. Aus diesem Grunde hat sich der Bundesgesetzgeber 2012 entschlossen, mit einem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten das Potential der jüngeren technologischen Entwicklungen auch auf prozessualem Gebiet auszuschöpfen. Mit dem Gesetz sollen die Zugangshürden für die elektronische Kommunikation mit der Justiz bedeutend gesenkt und das Nutzervertrauen im Umgang mit dem neuen Kommunikationsweg gestärkt werden. Das Gesetz vom 10. Oktober 2013 (BGBl. I S. 3786) regelt Details der elektronischen Dokumente für alle Gerichtsbarkeiten (ohne Strafgerichtsbarkeit) und erlaubt gestufte Inkrafttretensregelungen durch die Länder.

Grundsätzlich ist die Förderung des elektronischen Rechtsverkehrs mit den Gerichten positiv zu bewerten. Jedoch ist aus Sicht des Datenschutzes in den Fällen, in denen eine Pflicht zur Einreichung elektronischer Dokumente geschaffen wird, eine korrespondierende Pflicht zum Schutz der übersandten Daten gegen unbefugte Kenntnisnahme sicherzustellen. Dies gilt umso mehr, als Rechtsanwälte und Behörden spätestens ab 2022 zur

Nutzung des elektronischen Rechtsverkehrs verpflichtet sind. Sie dürfen dann vorbereitende Schriftsätze einschließlich deren Anlagen nur noch als elektronisches Dokument einreichen. Sofern Nachrichten durch De-Mail (siehe Nr. 4.5) versandt werden, ist damit zunächst nur eine Transportverschlüsselung verbunden. Eine zusätzliche Ende-zu-Ende-Verschlüsselung ist jedoch möglich und sollte auch von Rechtsanwälten und Gerichten gefordert werden, da im Rahmen gerichtlicher Verfahren häufig sensible personenbezogene Daten übermittelt werden. Der Bürger muss sich grundsätzlich darauf verlassen können, dass Behörden und Rechtsanwälte seine Daten nicht ungeschützt über das Internet versenden.

Diese datenschutzrechtlichen Überlegungen haben im Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten keinen entsprechenden Niederschlag gefunden. Vor diesem Hintergrund wird der Landesbeauftragte die Erfahrungen, die Rechtsanwälte, Behörden und Gerichte mit dem elektronischen Rechtsverkehr in Sachsen-Anhalt machen, kritisch beobachten und ggf. Korrekturen anregen.

Das o. a. Gesetz ist nur eines von vielen Beispielen der letzten Jahre für die Einführung elektronischer Verfahren in der Justiz bzw. Rechtspflege. Weitere Beispiele der E-Justiz sind das Zentrale Vorsorgeregister und das Zentrale Testamentsregister bei der Bundesnotarkammer (Gesetz vom 22. Dezember 2010, BGBl. I S. 2255), die elektronische Antragstellung auf Erteilung eines Führungszeugnisses aus dem Bundeszentralregister (Gesetz vom 6. September 2013, BGBl. I S. 3556) oder das Datenbankgrundbuch (Gesetz vom 1. Oktober 2013, BGBl. I. S. 3719). Der Landesbeauftragte wünscht sich eine stärkere Beteiligung durch das Landesjustizministerium und äußert diese Erwartung auch mit Blick auf § 14 Abs. 1 Satz 2 und 3 DSG LSA.

8 Verfassungsschutz

8.1 Reform der Sicherheitsbehörden

Die Erkenntnisse über den rechtsextremistischen Nationalsozialistischen Untergrund (NSU) haben dazu geführt, auch die Zusammenarbeit zwischen den Verfassungsschutzbehörden des Bundes und der Länder zu hinterfragen. Die Diskussion wurde und wird auch öffentlich geführt. Die Vorschläge gehen von einer Zentralisierung der Aufgaben des Verfassungsschutzes beim Bundesamt für Verfassungsschutz bis hin zur Auflösung aller Verfassungsschutzbehörden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit ihrer Entschließung anlässlich der 84. Konferenz im November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“ (**Anlage 18**) in die Diskussion eingebracht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darin Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen. Sie fordert die Bundesregie-

rung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Die Konferenz macht darüber hinaus darauf aufmerksam, dass bei einer Reform der Sicherheitsbehörden der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten sind.

Diese Auffassung unterstützt auch die Konferenz der Informationsfreiheitsbeauftragten in Deutschland mit ihrer Entschließung vom Juni 2013 „Transparenz bei Sicherheitsbehörden“. Sie unterstreicht, dass die Aufgaben und Befugnisse der Sicherheitsbehörden und deren tatsächliche Arbeitsweisen nachvollziehbar sein müssen und unterstützt die Stärkung der parlamentarischen Kontrolle.

Als eine Reaktion auf die Erkenntnisse zum NSU wurde auf Bundesebene bereits im Dezember 2011 das „Gemeinsame Abwehrzentrum gegen Rechtsextremismus“ eingerichtet. Das Zentrum dient als Informations- und Kommunikationsplattform für die Beteiligten. Auf Länderebene sind die Landeskriminalämter und die Verfassungsschutzbehörden beteiligt, auf Bundesebene sind es das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, die Bundespolizei, der Generalbundesanwalt und der Militärische Abschirmdienst. Darüber hinaus ist das Europäische Polizeiamt beteiligt (vgl. auch Nr. 5.3).

Auch die Ständige Konferenz der Innenminister und -senatoren der Länder hat sich anhand von Grundsatzpapieren und Kommissionsberichten mit Fragen nach der Neuausrichtung des Verfassungsschutzes beschäftigt. Tendenziell führen die Beschlüsse zu einem verstärkten wechselseitigen Informationsaustausch zwischen den Sicherheitsbehörden des Bundes und der Länder. Dabei soll der Bundesebene eine koordinierende Rolle zukommen. Darüber hinaus sollen sich der Einsatz von V-Leuten an bundesweit einheitlichen Kriterien ausrichten und die parlamentarische Kontrolle sowie die Transparenz gegenüber der Öffentlichkeit verstärkt werden.

Der Landesbeauftragte wird als Teil der Kontrolle über die Verfassungsschutzbehörde des Landes Sachsen-Anhalt die Entwicklungen zur Reform weiter begleiten und kommentieren. Der Landesinnenminister hat im Rahmen eines Acht-Punkte-Programms vom Herbst 2012 u. a. eine größere Transparenz des Verfassungsschutzes versprochen; offenbar in Anlehnung an eine neue Bund-Länder-Philosophie des Verfassungsschutzes als Informationsdienstleister und Partner in der Mitte der Gesellschaft. Allerdings wird die neue Transparenz bislang nur als Öffentlichkeitsarbeit praktiziert.

Ein im Rahmen einer „Neuordnung“ geplantes gemeinsames Sicherheitszentrum von Verfassungsschutz und Polizei ist noch vage geblieben. Ohnehin ist ein solches Vorhaben rechtsstaatlich angreifbar.

8.2 Moratorium bei Aktenvernichtung und Löschung von Daten

Wegen der Erkenntnisse zum NSU hat der Deutsche Bundestag im Januar 2012 einen Untersuchungsausschuss eingesetzt. „Der Untersuchungsausschuss soll sich ein Gesamtbild verschaffen zur Terrorgruppe ‚Nationalsozialistischer Untergrund', ihren Mitgliedern und Taten, ihrem Umfeld und ihren Unterstützern sowie dazu, warum aus ihren Reihen so lange unerkannt schwerste Straftaten begangen werden konnten. Auf der Grundlage der gewonnenen Erkenntnisse soll der Untersuchungsausschuss Schlussfolgerungen für Struktur, Zusammenarbeit, Befugnisse und Qualifikation der Sicherheits- und Ermittlungsbehörden und für eine effektive Bekämpfung des Rechtsextremismus ziehen und Empfehlungen aussprechen." (BT-Drs. 17/8453). Im Rahmen seiner Tätigkeit hat sich der Bundestagsuntersuchungsausschuss auch an die Verfassungsschutzbehörde des Landes Sachsen-Anhalt gewandt. Die Verfassungsschutzbehörde sollte sächliche Beweismittel, insbesondere Akten, die den Untersuchungsgegenstand betreffen, vorlegen.

In der Folge dieses Ersuchens musste die Frage geklärt werden, welche Unterlagen dem Bundestagsuntersuchungsausschuss vorgelegt werden können. Die datenschutzrechtlich zentrale Frage dabei ist, wie mit Daten umzugehen ist, die nach den Vorschriften des Verfassungsschutzgesetzes zu löschen wären. Diese Frage ist aber nicht einfach zu beantworten. Die Verpflichtung zum Löschen von Daten und Vernichten von Akten steht dem Interesse an der Unterstützung der Arbeit des Bundestagsuntersuchungsausschusses und der Aufklärung der Vorgänge um den Nationalsozialistischen Untergrund entgegen. Natürlich ist man verleitet festzustellen, dass die Aufklärung der Vorkommnisse durch den Untersuchungsausschuss Vorrang haben muss. Die entsprechende Interpretation der bestehenden Rechtslage erscheint dem Landesbeauftragten aber nicht zwangsläufig. Vor diesem Hintergrund hat der Landesbeauftragte das Gespräch mit dem Ministerium für Inneres und Sport gesucht und an einer datenschutzrechtliche Anforderungen berücksichtigenden Lösung mitgearbeitet.

Fakten waren zu diesem Zeitpunkt allerdings schon insoweit geschaffen, als die Verfassungsschutzbehörde bereits vor diesem Gespräch angewiesen wurden war, bis auf Weiteres auf das Löschen von Daten bzw. auf das Vernichten von Unterlagen zu verzichten (ähnlich im Polizeibereich). Wie durch entsprechende Presseberichterstattung bereits öffentlich bekannt wurde, hat die Verfassungsschutzbehörde große Teile ihrer Aktenbestände für eine Volltextrecherche nach Hinweisen auf die Terrorgruppe „Nationalsozialistischer Untergrund" digitalisiert. Ein solcher zweckgebunden gebildeter spezieller Datenbestand muss nach Wegfall der Zweckbestimmung auch wieder gelöscht werden. Hierüber besteht Einvernehmen zwischen dem Innenminister und dem Landesbeauftragten.

Der Landesbeauftragte wird das weitere Vorgehen in Bezug auf den vorübergehenden Verzicht auf Löschung und Vernichtung weiter begleiten. Grundsätzlich sind die personenbezogenen Daten zu löschen, wenn sie

zum Zweck der Gewinnung von Erkenntnissen für den Bundestagsuntersuchungsausschuss (Abschlussbericht in BT-Drs. 17/14600) oder für entsprechende konkrete Anfragen auf Landesebene nicht mehr benötigt werden. Die Verfassungsschutzbehörde teilte nach Abschluss ihrer Auswertung bereits mit, dass die Terrorgruppe NSU keine Strukturen und keine konkreten Verbindungen in bzw. nach Sachsen-Anhalt gehabt habe.

8.3 Anbietungspflicht an das Landeshauptarchiv

Mit einer Pressemitteilung vom 16. Januar 2013 (Nr. 005/2013) hat das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt den Vorwurf, Akten des Verfassungsschutzes seien unrechtmäßig vernichtet worden, zurückgewiesen. Vorausgegangen war dieser Erklärung die Äußerung eines Mitgliedes des Landtages von Sachsen-Anhalt, es seien jahrelang Akten ohne Rechtsgrundlage vernichtet worden (vgl. auch zur Rechtspraxis LT-Drs. 6/1726 und 6/1832).

Kernpunkt der Vorhaltungen ist die Frage nach der Anbietungspflicht des Verfassungsschutzes gegenüber dem Landeshauptarchiv. Nach § 9 Abs. 1 ArchG-LSA haben die Verfassungsorgane, Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Sachsen-Anhalt „… alle Unterlagen, sobald sie diese zur Erfüllung ihrer öffentlichen Aufgaben nicht mehr benötigen, unverzüglich, spätestens 30 Jahre nach der letzten inhaltlichen Bearbeitung, dem zuständigen Landesarchiv im Originalzustand zur Übergabe anzubieten und, wenn es sich um archivwürdige Unterlagen handelt, als Archivgut zu übergeben."

Die Diskussion um die grundsätzliche Anbietungspflicht der Verfassungsschutzbehörde wurde im März 2013 in nichtöffentlicher Sitzung des Ausschusses für Inneres und Sport des Landtages von Sachsen-Anhalt geführt. Der Landesbeauftragte war daran beteiligt und machte deutlich, dass nicht nur das ArchG-LSA und das VerfSchG-LSA (insbesondere § 11 Abs. 2 Satz 2) zu bewerten seien. Auch die Aktenordnung und die Verschlusssachenanweisung für das Land Sachsen-Anhalt müssen in die Betrachtung einbezogen werden.

Nach Kenntnisstand und mit Unterstützung des Landesbeauftragten wird seitens der Landesregierung an einem Gesetzentwurf gearbeitet, der inhaltliche Spannungsfelder zwischen dem ArchG-LSA und dem VerfSchG-LSA in Bezug auf die Archivierung von Unterlagen des Verfassungsschutzes auflösen soll.

8.4 Änderung des Verfassungsschutzgesetzes

In seinem X. Tätigkeitsbericht (Nr. 26.1) hat der Landesbeauftragte über Änderungen des VerfSchG-LSA berichtet. Die letzte dort geschilderte Änderung bezog sich auf das „Zweite Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt" aus dem Jahr 2010 (GVBl. LSA 2010 S. 541). Seither wurde das Gesetz wiederholt geändert.

Zunächst wurde das VerfSchG-LSA durch das „Dritte Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt“ vom 13. Juni 2012 (GVBl. LSA 2012 S. 187) geändert. Im Kern war die Änderung darauf gerichtet, den Einsatz des sog. IMSI-Catchers durch die Verfassungsschutzbehörde nunmehr dauerhaft zu ermöglichen (Standortermittlung aktiv geschalteter Mobilfunkendgeräte und Ermittlung der Geräte- und Kartennummer). Nach bis dahin geltender Rechtslage war die Regelung des § 17a Abs. 6 VerfSchG-LSA, die den Einsatz des IMSI-Catchers zuließ, zeitlich befristet. Zum 30. Juni 2012 sollte die Regelung außer Kraft treten. Zuvor war gesetzlich zum 31. Dezember 2011 eine Evaluierung der Regelungen zum IMSI-Catcher vorgesehen. Die Evaluierung wurde vorgenommen und dem Landtag von Sachsen-Anhalt vorgelegt (LT-Drs. 6/998). Im Evaluierungsbericht wird ausgeführt: „Zusammenfassend lässt sich feststellen, dass die Befugnis gemäß § 17a Abs. 6 VerfSchG-LSA zum Einsatz eines IMSI-Catchers sich in der Praxis bewährt hat. Die Regelung ist zur effektiven Aufgabenwahrnehmung des Verfassungsschutzes dieses Landes unverzichtbar und sollte deshalb beibehalten werden.“ Allerdings erfolgte die Evaluierung durch die Verfassungsschutzbehörde selbst und nur aufgrund eines Anwendungsfalles. Auf die Beteiligung externen Sachverstandes wurde verzichtet. Entsprechende Anmerkungen des Landesbeauftragten im Gesetzgebungsverfahren und sein Hinweis, dass Evaluierungen in transparenten Verfahren durch unabhängige Expertengremien die Objektivität der Evaluierung erhöhen können, führten letztendlich aber nicht zu einer Änderung des Gesetzentwurfes.

Positiv hervorzuheben ist der Umstand, dass eine Regelung zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung nicht im VerfSchG-LSA aufgenommen wurde. Eine auch in Sachsen-Anhalt im Jahre 2011 geführte Diskussion (vgl. X. Tätigkeitsbericht, Nr. 20.2) zum Einsatz von „Staatstrojanern“ (siehe zur Praxis LT-Drs. 6/588, 6/589, 6/590) ergab Einvernehmen zwischen dem Landesinnenminister und dem Landesbeauftragten, dass das G 10-Gesetz Überwachungen von Telefonaten über das Internet nicht zulässt; somit finden diese in Sachsen-Anhalt nicht statt (vgl. auch Nr. 7.1).

Der Entwurf eines „Vierten Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt“ (LT-Drs. 6/1569), der auf die Stärkung der Rechte der Parlamentarischen Kontrollkommission gerichtet war, wurde vom Landtag von Sachsen-Anhalt nicht beschlossen.

Durch Art. 2 des Gesetzes zur Neuregelung der Erhebung von telekommunikations- und telemedienrechtlichen Bestandsdaten vom 10. Oktober 2013 (GVBl. LSA S. 494) wurde das VerfSchG-LSA erneut geändert. Mit den Änderungen in § 17a VerfSchG-LSA wurde eine spezielle Rechtsgrundlage für das Einholen von Auskünften über Bestandsdaten bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, geschaffen. Anlass für diese Änderung war die Entscheidung des Bundesverfassungsgerichtes vom 24. Januar 2012 (BVerfGE 130, 151), zu der unter Nr. 4.13 näher ausgeführt wird. Auch durch den Vortrag des Landesbeauftragten konnte eine Änderung des ursprüngli-

chen Gesetzentwurfes dahingehend erreicht werden, dass über den Einsatz dieses Mittels der Landtag regelmäßig unterrichtet werden muss. Die seitens des Landesbeauftragten angeregte Aufnahme von Evaluierungsklauseln fand jedoch keinen Eingang.

9 Forschung, Hochschulen und Schulen

9.1 Forschung

9.1.1 Allgemeines

Im Berichtszeitraum wurden dem Landesbeauftragten 13 neue Forschungsvorhaben zur datenschutzrechtlichen Prüfung vorgelegt. Darüber hinaus fanden im Berichtszeitraum bei laufenden Projekten, wie z. B. bei der Internationalen Grundschul-Lese-Untersuchung (IGLU), der Internationalen Mathematik- und Naturwissenschaftsstudie (TIMSS), der Studie zur Entwicklung von Ganztagsschulen (StEG) und beim Nationalen Bildungspanel (NEPS), weitere Erhebungswellen statt, bei denen der Landesbeauftragte erneut aufwendig beteiligt wurde.

9.1.2 Nationale Kohorte

Bei der Nationalen Kohorte handelt es sich um eine Langzeitstudie, die chronische Erkrankungen erforschen soll. Geplant ist, 200.000 Studienteilnehmer nicht nur einmal zu untersuchen und zu befragen, sondern auch regelmäßige Nachuntersuchungen durchzuführen. Die Befragungen umfassen Informationen zum Gesundheitszustand, Lebensstil und Erkrankungen des Teilnehmers und dessen Familie. Die Untersuchungen beziehen sich u. a. auf die Messung von Gewicht, Größe und Blutdruck, EKG und Lungenfunktionstest, aber auch die Entnahme von Blut-, Urin- und Speichelproben.

Verantwortlich für die Durchführung der Studie ist der Verein „Nationale Kohorte e. V.“ 18 Studienzentren sind zuständig für das Probandenmanagement und die Durchführung der Untersuchungen. Ein Studienzentrum ist die Medizinische Fakultät der Martin-Luther-Universität Halle-Wittenberg. Die erhobenen Daten werden in pseudonymisierter Form in einer zentralen Datenbank gespeichert. Diese wird in zwei sog. Integrationszentren vorgehalten. Für die Befundung von Bildern oder EKG sind mehrere fachspezifische Kompetenzzentren zuständig. Darüber hinaus ist eine Treuhandstelle für die Verwaltung personenidentifizierender Daten und deren zugeordneter Pseudonyme verantwortlich. Ein Transferzentrum übermittelt die pseudonymisierten Daten an interne und externe Forscher.

Die lokalen Studienzentren erhalten auf Anfrage bei den Meldebehörden eine Zufallsstichprobe der Einwohner mit den persönlichen Daten (Name, Vorname, Geburtsdatum, Geschlecht, Adresse und Nationalität). Die potentiellen Teilnehmer werden angeschrieben und um deren Einwilligung gebeten. Die Teilnahme an der Studie erfolgt nach Aufklärung und Einwilligungserklärung freiwillig. Die Teilnehmer werden dann befragt und untersucht. Mit einem weiteren Einverständnis werden darüber hinaus weitere

Daten der Teilnehmer von Dritten erhoben (z. B. Rentenversicherungs- und Krankenkassendaten, Krebsregisterdaten).

Nach Erörterungen im Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit das Datenschutzkonzept positiv bewertet. Allerdings obliegt es den Datenschutzbeauftragten der Länder weiterhin, die Datenerhebung und -verarbeitung vor Ort in den lokalen Studienzentren datenschutzrechtlich zu prüfen und zu bewerten.

Im März 2013 legte die Martin-Luther-Universität Halle-Wittenberg erste Unterlagen für eine datenschutzrechtliche Prüfung vor. Insbesondere die im Studienzentrum getroffenen technisch-organisatorischen Maßnahmen nach § 6 DSG LSA werden noch geprüft.

9.1.3 INDECT – Forschung im Sicherheitsbereich

In den letzten Jahren mussten die Datenschutzbeauftragten des Bundes und der Länder zunehmend zur Kenntnis nehmen, dass mit öffentlichen Mitteln Forschungsprojekte gefördert wurden, die mit Hilfe von automatisierten Verfahren menschliche Verhaltensweisen analysieren.

So wurde z. B. durch die Europäische Union das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung) seit 2009 gefördert. Ziel dieses Projektes ist es, durch die Bündelung von Hard- und Software verschiedener Überwachungstechnologien bewegliche Objekte und Personen beobachten zu können. Verschiedene Daten, wie Kommunikationsdaten, Daten aus Überwachungskameras, der Handyortung usw., werden in Datenbanken zusammengeführt, wodurch Menschen, die einmal durch ihr „ungewöhnliches“ Verhalten „auffällig“ wurden, leichter überwacht werden können.

Das Projekt „INDECT“ sollte zur Fußball-EM 2012 in Polen erstmals getestet werden. Konkrete Datenschutzbestimmungen zu diesem Projekt konnten jedoch nicht geprüft werden, weil sie nicht bekanntgemacht wurden. Selbst in Mitteilungen der Europäischen Kommission wurde der Verdacht nicht ausgeräumt, dass die aktuellen Datenschutzbestimmungen zu diesem Projekt Besorgnis erregend seien.

Aus diesem Grund und weil mittlerweile auch das Rahmenprogramm der Europäischen Kommission für Forschung und Innovation „Horizont 2020“ für den Zeitraum 2014-2020 vorliegt, fassten die Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 83. Konferenz vom 21. bis 22. März 2012 in Potsdam eine mahnende Entschließung „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“ (**Anlage 10**), welche auch in der englischen Fassung an die Europäische Kommission weitergeleitet wurde.

9.2 Geburtsdatum in online-Veröffentlichung der Dissertation

Ein Petent beklagte, dass eine Universität nicht bereit war, die online gestellte Dissertation dahin zu ändern, dass das Geburtsdatum und der Geburtsort nicht mehr in der PDF-Datei erscheinen.

Das Vorgehen der Universität war aber aus datenschutzrechtlicher Sicht zulässig. Auf der Grundlage des § 18 Abs. 7 HSG LSA konnte die Universität Promotionsordnungen erlassen. Die Promotionsordnung sah in § 7 Abs. 6 vor, dass das Titelblatt der Dissertation auch Angaben zur Person aufweist, die in § 5 aufgeführt sind. Nach § 5 Nr. 6 der Promotionsordnung gehören zu den Angaben u. a. auch das Geburtsdatum und der Geburtsort. Im Hinblick auf künftige Identifikationen erschien zumindest die Aufnahme des Geburtsdatums wohl geboten. Insgesamt entsprach das Vorgehen auch akademischen Traditionen. Insoweit waren letztlich keine durchgreifenden Bedenken ersichtlich. Hinzu kam, dass der Petent die Online-Veröffentlichung der Promotion genehmigt hatte.

Problematisch wäre lediglich die Internetveröffentlichung von Lebensläufen gewesen, da insoweit die Aspekte der Erforderlichkeit der Datenverarbeitung einerseits und die im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigenden schutzwürdigen Interessen der Betroffenen eine Unzulässigkeit nahe gelegt hätten.

9.3 Datenschutz in Schulen

Der Landesbeauftragte hat in diesem Berichtszeitraum erneut Schulen hinsichtlich der Einhaltung der datenschutzrechtlichen Vorschriften geprüft.

Erneut war festzustellen, dass keine behördlichen Datenschutzbeauftragten nach § 14a DSG LSA bestellt waren, obwohl automatisierte Datenverarbeitungsverfahren verwendet werden (vgl. X. Tätigkeitsbericht, Nr. 21.3). Da dies bisher leider beständig festzustellen war, hat der Landesbeauftragte eine landesweite Schulumfrage gestartet (siehe Nr. 9.3.1).

Außerdem haben die Schulleitungen selten Genehmigungen zur Verarbeitung personenbezogener Schülerdaten auf privaten Lehrerrechnern erteilt, Aufbewahrungsfristen wurden nicht kontrolliert oder Klassenbücher und Notenhefte wurden nicht verschlossen aufbewahrt.

Der Landesbeauftragte hat den Schulen entsprechende datenschutzrechtliche Hinweise gegeben.

9.3.1 Behördliche Datenschutzbeauftragte in Schulen

Die gesetzliche Bestellungsverpflichtung für behördliche Datenschutzbeauftragte besteht bereits seit 2001. Dies war Anlass, im Zeitraum von November 2011 bis März 2012 eine Stichprobe von landesweit zufällig ausgewählten Grund- und Sekundarschulen, Gymnasien, Gesamtschulen und

Berufsbildenden Schulen anzuschreiben und um Übersendung einer Bestellungsurkunde des behördlichen Datenschutzbeauftragten zu bitten.

Das Ergebnis dieser Befragung stellt sich zusammenfassend wie folgt dar:

	Grundschulen	**weiterführende Schulen**
angeschrieben	58	31
geantwortet	52	19
davon:		
bereits zuvor bestellte bDSB	0 %	5 %
Bestellung eines eigenen bDSB nach LfD-Kontakt	73 %	53 %
Bestellung eines externen bDSB nach LfD-Kontakt	12 %	0 %
keine Bestellung erfolgt	15 %	42 %

Aufgrund dieser Ergebnisse wurden folgende Bewertungen vorgenommen:

Nach dem Versand der Anfrage entstand ein enormer, zunächst telefonischer, später aber auch schriftlicher Beratungsbedarf bei den Schulen. Mitarbeiter des Landesbeauftragten haben u. a. an einer Schulleiterdienstberatung teilgenommen.

Die Mehrheit der Schulen hatte sich zuvor noch nicht mit den Vorschriften des DSG LSA und somit auch nicht mit der Bestellungsverpflichtung beschäftigt. Die Fragen richteten sich hauptsächlich auf die Voraussetzungen für eine Bestellung und die Anforderungen und Aufgaben eines behördlichen Datenschutzbeauftragten.

Die Rückmeldungen der Schulen erfolgten ziemlich schleppend. Trotz mehrfacher Erinnerungen konnte vor allem im Bereich der weiterführenden Schulen eine nur inakzeptable Rücklaufquote erreicht werden (60 %). Dies ist ein vielfach eklatanter Verstoß gegen die gesetzliche Verpflichtung zur Unterstützung des Landesbeauftragten gem. § 23 Abs. 1 DSG LSA.

Beachtlich ist auch, dass von den insgesamt 89 angeschriebenen Schulen lediglich eine Sekundarschule bereits einen behördlichen Datenschutzbeauftragten bestellt hatte. Die Bestellungsurkunde liegt vor. Aufgrund der dortigen Angaben war jedoch festzustellen, dass die Bestellung in keiner Weise den Anforderungen des § 14a DSG LSA entsprach.

Dies war leider ebenso bei den Bestellungen festzustellen, die nach dem Anschreiben des Landesbeauftragten erfolgten. Vielfach wurde die Bestellung nach BDSG und nicht nach DSG LSA durchgeführt oder die Schullei-

tung bestellte sich selbst zum behördlichen Datenschutzbeauftragten. Entsprechend war auch hier eine große Unsicherheit der Schulleitungen bei der Anwendung datenschutzrechtlicher Vorschriften zu erkennen, die in den vorliegenden Einzelfällen durch Beratungsangebote mutmaßlich behoben werden konnte.

Besonders auffällig ist ebenfalls die hohe Zahl der „Verweigerer“, d. h. die Schulen, die aus ihrer Sicht trotz Mahnung und Beratung nicht bereit oder in der Lage waren, ihren gesetzlichen Verpflichtungen nachzukommen. Die Erklärungen hierfür werden beispielhaft dargestellt:

Einige Schulen erklärten, keine automatisierten Verfahren zu verwenden, sodass keine Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten besteht. Diesbezüglich wurden sogar schulfachliche Referenten im damals noch zuständigen Landesverwaltungsamt und das Kultusministerium beteiligt. Das Kultusministerium beriet die Schulen dahingehend, dass die Bestellung eines behördlichen Datenschutzbeauftragten nur erforderlich sei, „wenn abweichend von der Regel automatisierte Verfahren eingesetzt und diese über die in § 14 Abs. 4 benannten Verfahren hinausgehen“. Eine Beteiligung des Landesbeauftragten erfolgte nicht. Jede Schulverwaltungssoftware stellt jedoch ein Verfahren nach § 2 Abs. 2 DSG LSA dar. Die Daten werden in einer Eingabemaske erfasst, i. d. R. in einer Datenbank gespeichert und können für verschiedene Zwecke ausgewertet werden. Allenfalls die Nutzung von Word- oder Excel-Dateien könnte als Verfahren gem. § 14 Abs. 4 Satz 2 DSG LSA betrachtet werden. Es ist daher eher die Regel, dass Schulen automatisierte Verfahren verwenden und somit einen behördlichen Datenschutzbeauftragten zu bestellen haben.

Die Mehrheit der Schulen gab organisatorische Probleme bei der Bestellung eines behördlichen Datenschutzbeauftragten an. So sei kein dafür qualifiziertes Personal vorhanden oder ausreichende Arbeitszeit stünde nicht zur Verfügung. Oft wurde auf fehlende Anrechnungsstunden verwiesen.

Infolge großflächiger Missachtung gesetzlicher Verpflichtungen bestand daher erheblicher Handlungsbedarf. Der Landesbeauftragte hat deshalb im Mai 2012 das Kultusministerium eindringlich gebeten, Maßnahmen zur Gewährleistung des Datenschutzes an den Schulen vorzunehmen, und im Rahmen seiner schmalen personellen Kapazitäten seine Unterstützung angeboten.

Im Oktober 2012 teilte der Kultusminister mit, alle Schulleitungen in Sachsen-Anhalt anschreiben zu wollen, um auf die geltende Rechtslage aufmerksam zu machen. Die Auffassung, dass der Einsatz einer Schulverwaltungssoftware an einer Schule ein automatisiertes Verfahren nach § 2 Abs. 2 DSG LSA darstellt und somit die Bestellung eines behördlichen Datenschutzbeauftragten erforderlich macht, werde geteilt. Die notwendigen Schritte, um bis zum Schuljahresbeginn 2012/2013 mit dem Landesschulamt zu einem abgestimmten Verfahren zu gelangen, seien veranlasst und

man werde auf die angebotene Hilfe des Landesbeauftragten zurückkommen.

Weitere Kontrollen bestätigten den fortwährenden Mangel an Bestellungen von behördlichen Datenschutzbeauftragten in Schulen. Das Kultusministerium verwies auf Nachfragen des Landesbeauftragten vom März und Juli 2013 darauf, dass eine Regelung zu schulischen Datenschutzbeauftragten leider erst in einer zukünftig geplanten Datenschutzverordnung in Ausfüllung der neuen Schulgesetznormen (siehe Nr. 9.4) vorgesehen sei.

9.3.2 Meldung besonderer Vorkommnisse an Landesschulamt

Mit Runderlass vom 30. Juli 2007 hat das Kultusministerium das Verhalten von Schulen bei Schadensereignissen und Bedrohungslagen geregelt. Unter anderem ist in Nr. 8 des Erlasses vorgeschrieben, dass besondere Ereignisse, die den Schulbetrieb gefährden, behindern oder verhindern oder die Unterstützung der Schulaufsicht oder den schulpsychologischen Dienst erfordern oder zu einem Eingriff weiterer Behörden führen, sofort telefonisch und im Nachgang mittels vorgegebenen Formulars dem Landesschulamt zu melden sind. Das Landesschulamt informiert über gravierende Vorkommnisse das Kultusministerium.

Um zu ermitteln, ob und in welchem Umfang auch personenbezogene Daten von Schülern und Lehrern in diesen Meldungen enthalten sind, hat der Landesbeauftragte im Mai 2012 Meldungen aus den Jahren 2009, 2011 und 2012 durchgesehen und festgestellt, dass nahezu in allen Meldungen die betroffenen Schüler und Lehrer namentlich aufgeführt waren. Es handelte sich z. B. um mit Hepatitis B infizierte Schüler, Hakenkreuzschmierereien, von Schülern angekündigte Amokläufe, eine Schlägerei auf dem Schulgelände.

Grundsätzlich schienen die Vorgänge jedoch lediglich informatorischen Charakter zu haben. In den vom Landesbeauftragten eingesehenen Meldungen waren keine Anhaltspunkte dafür erkennbar, dass das Landesschulamt oder das Kultusministerium unterstützend oder anderweitig tätig geworden wären. Die Erforderlichkeit der namensbezogenen Meldung war in keinem Fall ersichtlich. Der Landesbeauftragte hat daher gefordert, nur dann namensbezogene Meldungen vorzunehmen, wenn dies in begründeten Einzelfällen erforderlich ist. Auf das Gebot der Datensparsamkeit und Datenvermeidung wurde hingewiesen.

Darüber hinaus waren die Aufbewahrungsfristen dieser Unterlagen im Landesschulamt nicht bekannt. Im Hinblick auf die gesetzlichen Vorgaben wurde das Landesschulamt ergänzend gebeten, Aufbewahrungsfristen konkret festzulegen und die betroffenen Mitarbeiter unbedingt entsprechend zu informieren.

Auch nach mehrmaliger schriftlicher und telefonischer Erinnerung war bisher keine Rückäußerung des Landesschulamtes zu verzeichnen. Dass zunächst „vorsorglich“ namensbezogen gemeldet wurde, erscheint zumindest nachvollziehbar, die Verweigerung einer Stellungnahme als Verstoß

gegen die Unterstützungspflicht gegenüber dem Landesbeauftragten nach § 23 Abs. 1 Satz 1 DSG LSA dagegen nicht.

9.4 Änderung des Schulgesetzes – gläserner Schüler

Über das Vorhaben der Kultusministerkonferenz, einen sog. Kerndatensatz schulstatistischer Individualdaten einzuführen, und die diesbezüglichen Bedenken hatte der Landesbeauftragte bereits im VIII. Tätigkeitsbericht (Nr. 19.1) informiert. Dann rückten landesinterne Aktivitäten in den Vordergrund. Unter der Überschrift der Anschaffung einer einheitlichen Schulverwaltungssoftware wurde die Anlegung zentraler operativer Datenbanken mit Identifikationsnummern zu Schülerinnen und Schülern vorbereitet. Dies sollte schulübergreifenden Verwaltungszwecken dienen. Gleichzeitig sollte der Umfang der Verwaltungsdaten die Zusammenführung hinreichender Informationen für Planungs- und Statistikzwecke ermöglichen und weiterhin auch gewährleisten, dass aus dem Bestand die Generierung des sog. Kerndatensatzes zum einzelnen Schüler möglich ist. Hierzu hatte der Landesbeauftragte im IX. Tätigkeitsbericht (Nr. 20.3) ausgeführt.

In der Vergangenheit hatte der Landesbeauftragte stets auf grundlegende Aspekte hingewiesen. Dazu gehörte die Regelung wesentlicher Fragen durch den Gesetzgeber selbst, insbesondere vor dem Hintergrund der beabsichtigten Streubreite und des damit verbundenen erheblichen Grundrechtseingriffs durch die zentrale Erfassung aller Schülerinnen und Schüler. Das verfassungsrechtliche Erforderlichkeitsprinzip wurde ebenso betont wie die verfassungsrechtlich gebotene Trennung von Statistik und Verwaltung. Eine differenzierte gesetzliche Regelung wurde angemahnt. Diese Problematik wurde im X. Tätigkeitsbericht (Nr. 21.4) angesprochen. In der Stellungnahme der Landesregierung sagte der Kultusminister zu, den Landesbeauftragten in einer Arbeitsgruppe angemessen zu beteiligen.

Daran, sowie an die Vorgabe der Beteiligung nach § 14 Abs. 1 Satz 3 DSG LSA, musste der Landesbeauftragte erinnern, als er kurzfristig erfuhr, dass die Landesregierung einen Entwurf zur 14. Änderung des Schulgesetzes des Landes Sachsen-Anhalt beschlossen und zur Anhörung freigegeben hatte. Auf die vielfältigen datenschutzrechtlichen Unzulänglichkeiten konnte der Landesbeauftragte in nun wieder aufgenommenen Beratungen mit dem Kultusministerium und in einer Anhörung des Ausschusses für Bildung und Kultur des Landtages von Sachsen-Anhalt zum Gesetzentwurf (LT-Drs. 6/1165) hinweisen.

In mühevoller Detailarbeit mussten die ursprünglichen Formulierungen hinsichtlich ihrer Bedeutung und der Zusammenhänge hinterfragt und auf Unstimmigkeiten hingewiesen werden. Infolge einer nur knappen und nicht auf die einzelne Regelung bezogenen Begründung waren weitere Erläuterungen zum Verständnis erforderlich. Letztlich konnte der Landesbeauftragte in dann fruchtbarer Zusammenarbeit an der Erarbeitung eines Vorschlags für einen Änderungsantrag (vgl. LT-Drs. 6/1593) beratend mitwir-

ken. Auch bei diesen Beratungen stand das **Gebot der Trennung von Statistik und Verwaltung** im Vordergrund. Die statistikrechtlich gebotene Abschottung war zu gewährleisten. Es wurde darauf gedrungen, dass die Handelnden dem strafrechtlich sanktionierten Statistikgeheimnis unterliegen.

Weiter wurde betont, schon gesetzlich festzulegen, welche Daten für welche Zwecke Verwendung finden sollen. Während in einzelnen vom Ministerium dargestellten Beispielen die Notwendigkeit zentraler Aufgabenwahrnehmung und ein diesbezüglicher Datenbestand nachvollziehbar erschien, blieben bei anderen angedachten Verwendungen nicht unerhebliche Zweifel. Exemplarisch sind die in den abschließenden Formulierungsvorschlägen enthaltenen Merkmale der Schulpflicht zu nennen. Entgegen dem Wortlaut soll es sich hierbei ausdrücklich nicht um eine sog. „Schulschwänzerdatei“ handeln. Vielmehr soll im Schulleben u. a. beobachtet werden, ob die Mindestschulbesuchszeit eingehalten wird oder die Schulwechsel ordnungsgemäß ablaufen.

Mit dem Aspekt der Erforderlichkeit korrespondiert das Verbot der Vorratsdatenspeicherung. Eine vorsorgliche, dauerhafte aktualisierte Sammlung umfassender Schülerdaten zu allenfalls bereichsmäßig benannten, aber nicht klar bestimmten Zwecken mit der Möglichkeit, sich nach Bedarf daraus zu bedienen, wäre nicht akzeptabel.

Weiter wurde der Aspekt einer landeseindeutigen Schüler-Identifikationsnummer problematisiert, die die Durchführung schulübergreifender Aufgaben erleichtern solle und die Datenqualität verbessern helfe. Auch insoweit stellte sich die Frage der Erforderlichkeit. Es ergaben sich Bedenken, dass dieses Merkmal zu Verknüpfungen genutzt werden könnte, die wegen der Trennung von Statistik und Verwaltung unzulässig sind.

Im Hinblick auf den Kerndatensatz gab der Landesbeauftragte zu bedenken, dass eine **Totalerfassung** aller Schülerinnen und Schüler weiterhin **unverhältnismäßig** erscheine. Die Erforschung von einzelnen Zusammenhängen schulischen Lebens könne ggf. auch durch Studien erfolgen, wie dies bereits vielfach der Fall sei. Zudem müsse vermieden werden, dass sich aus den vorhandenen Daten infolge des Umfangs auch ohne Namenskenntnis auf den einzelnen Schüler oder die Schülerin zurückschließen lässt.

In den abschließenden Vorschlag für einen Änderungsantrag gingen vielfache Hinweise des Landesbeauftragten ein. Wesentliche, grundrechtsrelevante Belange sind gesetzlich festgelegt. So werden die Aufgabenbereiche, für die die Daten einer zentralen Schülerdatei verwendet werden dürfen, konkreter benannt. Die Stelle, die Schülerlaufbahnstatistiken für Planungszwecke erstellen soll, unterliegt den Grundsätzen des Landesstatistikgesetzes. Dies dient der Abschottung personenbezogener Daten der Statistik von der Schulverwaltung. Noch offene Detailfragen werden im Rahmen von Erörterungen zu künftigen Rechtsverordnungen zu diskutieren sein, deren Erlass vorgesehen ist (siehe §§ 84a bis f der Schulgesetz-

novelle vom 5. Dezember 2012, GVBl. LSA 2012 S. 560 – Neubekanntmachung des Gesetzes in GVBl. LSA 2013 S. 68). Damit wäre noch die Chance gegeben, die Verfassungskonformität der Regelungen zu stärken.

Denn einige grundlegende Bedenken bleiben bestehen, wie beispielsweise hinsichtlich einer statistischen Totalerfassung, die Sorge vor der Gefahr eines gläsernen Schülers sowie Zweifel an der Notwendigkeit einer zentralen Verwaltungsdatei, an der Notwendigkeit einer landeseinheitlichen Schülernummer und an der Anonymität des Kerndatensatzes. Die Entwicklung insbesondere in Bezug auf die zentrale Verwaltungsdatei und die Statistikerstellung bedarf der weiteren datenschutzrechtlichen Beratung und Begleitung.

9.5 Medienkompetenz

Auch in diesem Berichtszeitraum hat der Landesbeauftragte sowohl auf Landesebene als auch im Rahmen des Arbeitskreises Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Veranstaltungen und Planungen zur Stärkung der Medienkompetenz und des Datenschutzbewusstseins mitgewirkt.

Aufgrund der Aktualität des Themas haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 82. Konferenz am 28./29. September 2011 die Entschließung „Datenschutz als Bildungsaufgabe“ gefasst (**Anlage 4**). Die Datenschutzbeauftragten des Bundes und der Länder fordern weitergehende und nachhaltige Anstrengungen, um die Internetnutzer besser für ein selbstverantwortliches digitales Leben zu befähigen. Diesbezüglich wird u. a. darauf gedrängt, dass die Vermittlung von Medien- und Datenschutzkompetenz ausdrücklich in den Bildungsstandards und **Lehrplänen** verankert und zum verbindlichen Gegenstand der **Lehrerausbildung** gemacht wird.

Auch die Kultusministerkonferenz hat sich mit „Medienbildung in der Schule“ befasst und am 8. März 2012 einen entsprechenden Beschluss gefasst. Dieser soll dazu beitragen, dass Medienbildung als Pflichtaufgabe schulischer Bildung verankert wird und den Schulen und Lehrkräften Orientierung für die Medienbildung in Erziehung und Unterricht geben. Für die Kultusminister wäre z. B. die Aktualisierung und Akzentuierung der Medienbildung in den einzelnen Fächern wünschenswert. Außerdem ist Medienbildung in den Bildungswissenschaften, in der fachbezogenen Lehrerausbildung und in den Qualifizierungs- und Fortbildungsangeboten für Lehrkräfte zu verankern.

Bereits am 4. Mai 2010 wurde vom Deutschen Bundestag eine Enquete-Kommission „Internet und digitale Gesellschaft“ eingesetzt, die Handlungsempfehlungen zur Verbesserung der Rahmenbedingungen der Informationsgesellschaft vorlegen sollte. Sowohl die Projektgruppe Medienkompetenz als auch die Projektgruppe Datenschutz/Persönlichkeitsrechte erklären in ihren Berichten, dass die Ausbildung und Förderung von Medienkompetenz und Selbstdatenschutz von Nutzern digitaler Medien unverzichtbar ist (BT-Drs. 17/7286 und 17/8999; vgl. auch BT-Drs. 17/9246).

Datenschutz als Bildungsaufgabe soll auch in der Europäischen Datenschutz-Grundverordnung verankert werden; einem entsprechenden Vorschlag der Datenschutzkonferenz steht die Bundesregierung positiv gegenüber.

In Sachsen-Anhalt hat die Landesregierung im Februar 2011, wie bereits im X. Tätigkeitsbericht (Nr. 21.2) dargestellt, ein Konzept für die Stärkung der Medienkompetenz vorgelegt. Darin ist u. a. die Einrichtung der Arbeitsgruppe „Medienbildung/Medienkompetenz Sachsen-Anhalt“ vorgesehen. Die Arbeitsgruppe, deren Mitglied auch der Landesbeauftragte ist, versteht sich als Impulsgeber.

Sie hat u. a. beschlossen, einen Medienpass für Schüler einzuführen. Für Grundschulen und im Sekundarschulbereich sollen diesbezüglich verpflichtende Unterrichtsanteile eingeführt werden, die mit einer Prüfung enden. Zuständig für die Einführung und Betreuung des Medienpasses ist das Landesinstitut für Schulqualität und Lehrerbildung (LISA).

Durch die Schulverwaltung wurde auch festgelegt, dass für die Landkreise und kreisfreien Städte je ein medienpädagogischer Berater (0,5 Stelle) zur Verfügung stehen soll. Hierbei handelt es sich um Lehrkräfte, die u. a. die Schulträger und Schulen bei der Planung und Durchführung medienpädagogischer Angebote beraten und die aktive Medienbildungsarbeit in Schulen und kommunalen Einrichtungen fördern (Beginn in 2013).

Vor allem konnte erreicht werden, dass die bei der Landesmedienanstalt angesiedelte **Netzwerkstelle Medienkompetenz** ab 11. Juni 2012 ihre Arbeit aufnahm. Ziel dieses Projektes ist die Stärkung, Verknüpfung und der Ausbau von Aktivitäten im Bereich der Medienkompetenzförderung in Sachsen-Anhalt. Die Netzwerkstelle Medienkompetenz führt z. B. Regionalkonferenzen durch und hat einen medienpädagogischen Atlas mit Ansprechpartnern und Informationen aufgebaut.

Darüber hinaus war für 2013 in Zusammenarbeit zwischen der Landesmedienanstalt und dem Kultusministerium die Bereitstellung von Informationsbroschüren zum Thema Soziale Netzwerke und Datenschutz geplant. Diese wurde mittlerweile auf 2014 verschoben. Zielgruppe sollen zunächst die Lehrer sein.

Auf der ersten Netzwerktagung Medienkompetenz Sachsen-Anhalt im September 2011 diskutierten und berieten Vertreter aus verschiedenen Bereichen der Medien und Medienbildung über schulische Medienkompetenzvermittlung und medienpädagogische Angebote und deren Vernetzung. Der Landesbeauftragte hat an der Auftaktpodiumsdiskussion zum Thema „Wo steht Sachsen-Anhalt bei der Medienkompetenzvermittlung?“ und dem Panel „Total vernetzt! Risiken und Potentiale Sozialer Online-Netzwerke“ teilgenommen.

Im September 2013 hat die nächste Netzwerktagung stattgefunden, die sich der außerschulischen Medienbildung widmete; der Landesbeauftragte

beteiligte sich an einem Panel zu Fragen des Verbraucherdatenschutzes im Bereich der Familie.

Der Landtag hat im Rahmen der Erörterung des X. Tätigkeitsberichts des Landesbeauftragten wegen der besonderen Bedeutung des Medienkompetenzerwerbs die Landesregierung gebeten, die Umsetzung des o. g. Konzeptes zu intensivieren, um die Sensibilität junger Menschen im Umgang mit ihren persönlichen Daten zu stärken (LT-Drs. 6/1545, 6/1733).

Bei wesentlichen Schwerpunkten des Konzepts der Landesregierung fehlt es, wie ein Zwischenbericht nach zwei Jahren ausweist, an **Verbindlichkeit** und **Nachhaltigkeit**. Dies gilt insbesondere für die Verankerung der Medienbildung im Sinne eines fächerübergreifenden und fachintegrativen Ansatzes in den Lehrplänen aller Schulformen und Fächer, die Einbindung medienpädagogischer Pflichtmodule in die erziehungswissenschaftliche Grundlagenausbildung und die Ausweitung verbindlicher Fortbildungsangebote für die Lehrkräfte. Zusätzlich wären auch eine Aufwertung des Wahlpflichtfaches Moderne Medienwelten und die Verstärkung der Medienkompetenzmodule in allen Fachdidaktiken aller Lehramtsstudiengänge geboten, wenn nicht ein eigenes Pflichtfach eingerichtet wird. Zukünftig wird auch der außerschulische Bereich in den Blick kommen mit entsprechenden Maßnahmen: Jugendarbeit, Schulsozialarbeit, Medienbildung für Familien und Senioren, politische Bildung (vgl. auch **Anlage 41**).

10 Gesundheits- und Sozialwesen

10.1 Gesundheitswesen

10.1.1 Krankenhausinformationssysteme

Die Orientierungshilfe Krankenhausinformationssysteme wurde im X. Tätigkeitsbericht (Nr. 12.1) vorgestellt. Der Landesbeauftragte begleitet die weitere Entwicklung der Orientierungshilfe in der Unterarbeitsgruppe des Arbeitskreises Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Zudem hatte er Gelegenheit, die Orientierungshilfe den betrieblichen Datenschutzbeauftragten der Krankenhäuser im Rahmen einer Veranstaltung der Krankenhausgesellschaft Sachsen-Anhalt zu erläutern. Die Erfahrung in anderen Ländern hat gezeigt, dass die umfassende Digitalisierung der Datenverarbeitung und die notwendig schnelle und effiziente Kommunikation im Rahmen einer vernetzten Patientenbehandlung teilweise zu unsensiblem Umgang mit Patientendaten führten. Der Landesbeauftragten hat daher mit dem Besuch von Krankenhäusern begonnen, bei dem der datenschutzkonforme Umgang mit den Patientendaten anhand der Maßstäbe der Orientierungshilfe hinterfragt wird.

10.1.2 Medizinisches Versorgungszentrum

Die strukturierte, interdisziplinäre Versorgung gewinnt im Gesundheitswesen an Bedeutung. Die enge Kooperation und schnelle Kommunikation ist sowohl im ambulanten wie im stationären Bereich als auch zwischen die-

sen Bereichen zunehmend gefordert. In der vertragsärztlichen Versorgung sind Medizinische Versorgungszentren (MVZ) als fachübergreifende Versorgungsform vorgesehen. Zur Optimierung der Gesamtversorgung ist oft der schnelle Austausch von Behandlungsdaten der Patienten wünschenswert. Vielfach sind Ärztinnen und Ärzte sowohl in einem Krankenhaus als auch in einem Versorgungszentrum beschäftigt. Damit entsteht der Bedarf, auf die in der jeweils anderen Einrichtung erhobenen Daten für die weitere Behandlung zuzugreifen. Die in der Praxis inzwischen häufige Anbindung von MVZ an Kliniken bedarf jedoch der Berücksichtigung vielfacher Rahmenbedingungen, um dem Schutz des Persönlichkeitsrechts der Patienten Rechnung zu tragen.

Ein städtisches Klinikum beabsichtigte, eine gemeinsame elektronische Datenverarbeitung mit dem von ihm getragenen MVZ einzurichten. Hierzu konnte der Landesbeauftragte einige Hinweise geben. Die Beratungen werden fortgesetzt.

Das MVZ ist als gemeinnützige GmbH rechtlich selbständig. Aus datenschutzrechtlicher Sicht handelte es sich daher bei dem Klinikum und dem MVZ um zwei getrennt zu betrachtende verantwortliche Stellen (siehe § 3 Abs. 7 BDSG). Die jeweils andere Einrichtung ist Dritter im datenschutzrechtlichen Sinn. Der Transfer von Patientendaten stellt damit eine Übermittlung (§ 3 Abs. 4 Nr. 3 BDSG) dar und bedarf daher zunächst einer datenschutzrechtlichen Grundlage. Dies ergibt sich aus § 3 Abs. 2 Nr. 1 DSG LSA i. V. m. § 4 Abs. 1 BDSG für das Klinikum in Trägerschaft der Stadt, das als sog. Wettbewerbsunternehmen einzustufen ist (vgl. Nr. 3.2.1.1 VV-DSG-LSA). Für das MVZ folgt dies aus § 4 Abs. 1 BDSG. Zu beachten ist, dass Gesundheitsdaten nach § 3 Abs. 9 BDSG (ggf. i. V. m. § 3 Abs. 2 Nr. 1 DSG LSA) personenbezogene Daten besonderer Art sind. Als Rechtsgrundlage kommt insbesondere § 28 Abs. 6 und 7 BDSG in Betracht. Die Datenermittlung muss auf das jeweils im Einzelfall erforderliche Maß beschränkt sein. Zudem ist zu berücksichtigen, dass die Patientendaten durch die ärztliche Schweigepflicht nach § 203 StGB geschützt sind, sodass neben der datenschutzrechtlichen Rechtsgrundlage auch jeweils eine Offenbarungsbefugnis im Sinne von § 203 StGB vorliegen muss.

Grundsätzlich ist aufgrund der o. g. Vorgaben zunächst eine strikte Trennung der (elektronischen) Verwaltung der Behandlungsakten von Klinikum und MVZ geboten. Die Beziehung zwischen Klinikum und MVZ entspricht der von Klinikum zu anderen niedergelassenen Ärzten. Die Patientendaten von Klinikum und MVZ sind in separaten Mandanten zu verarbeiten. Pauschale Übermittlungen oder Abrufe bzw. die Einrichtung der Möglichkeit der Kenntnisnahme von Patientendaten der jeweils anderen Einrichtung sind grundsätzlich nicht ohne Weiteres zulässig.

Die Trennung ist auch für die Patienten deutlich erkennbar zu machen, um ihnen die Wahrnehmung ihrer Persönlichkeitsrechte gegenüber dem jeweiligen Partner zu gewährleisten (räumliche Distanz, Firmierung bzw. optischer Auftritt).

Als Grundlage für eine rechtliche Ausgestaltung der (elektronischen) Zusammenarbeit zwischen Klinikum und MVZ wird häufig die Rechtsfigur der Datenverarbeitung im Auftrag diskutiert. So wäre beispielsweise denkbar, dass das Klinikum bei Einhaltung der Vorgaben des § 11 BDSG für das MVZ auf seinen Rechnern die Patientendaten im Auftrag verarbeitet. Damit wäre das MVZ weiter die verarbeitende und datenschutzrechtlich verantwortliche Stelle, es läge keine Übermittlung vor, die einer datenschutzrechtlichen Grundlage bedürfte. Offen ist, ob die Ausgestaltung als Datenverarbeitung im Auftrag durch eine Einwilligung bzw. Entbindung von der Schweigepflicht jeweils im Einzelfall akzeptabel wäre. Die Situation des Hilfe suchenden Erkrankten in der Aufnahme stellt das Verständnis für die Rechtskonstruktion und die Annahme einer Freiwilligkeit als Grundlage in Frage. Zumindest müssten Alternativen angeboten werden.

Darüber hinaus ist aber zu beachten, dass auch das ärztliche Berufsgeheimnis betroffen ist. Eine Verarbeitung auf Rechnern der anderen Einrichtung wäre also auch eine Offenbarung, für die § 11 BDSG keine Befugnisnorm darstellt (§ 1 Abs. 3 Satz 2 BDSG).

Für eine Übermittlung zwischen den getrennten Einrichtungen bedürfte es grundsätzlich einer Einwilligung.

Die Tragfähigkeit einer denkbaren konkludenten Einwilligung in einen Datentransfer aufgrund von Informationen durch Aushang oder Auslage erscheint aus unterschiedlichen Gründen fraglich (u. a. Bestimmtheit, Beweislage). Ausnahmen können in Situationen gegeben sein, in denen bei objektiver Betrachtung davon auszugehen ist, dass der Patient mit der Weitergabe der Informationen einverstanden ist (Nachbehandlungen oder Konsilaufträge, die konkret geplant und erörtert sind; stationäre Aufnahme nach Einweisung durch das MVZ; Notsituationen).

Aufgrund der vielfältigen technischen Ausgestaltungsmöglichkeiten und der verschiedenen Behandlungssituationen sind diverse Transferszenarien denkbar. Ausgestaltungen müssen die Hoheit des Patienten in Bezug auf seine sensiblen Gesundheitsdaten beachten. Wesentliche Aspekte sind die möglichst konkrete Information des Patienten, die Bezeichnung der betroffenen Daten sowie die Beschreibung des Verfahrensweges, der Zugriffsberechtigten und der Verwendungszwecke. Die Rollen- und Berechtigungskonzepte möglicher Zugriffe müssen sich an der Erforderlichkeit orientieren.

Weiter ist bei der Ausgestaltung auf die Einhaltung der technisch-organisatorischen Anforderungen (§ 9 BDSG) zu achten. Neben gesicherten Datenwegen ist auch eine umfängliche Protokollierung erforderlich. Ergänzend sind Archivierungsfragen und die Notwendigkeit von Löschungen nach Ablauf der Aufbewahrungsfristen zu berücksichtigen.

Ein Szenarienkatalog zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern findet sich auf der Homepage des Landesbeauftragten.

10.1.3 Maßregelvollzug

Im X. Tätigkeitsbericht (Nr. 12.4) hatte der Landesbeauftragte über seine intensive Beteiligung bei der Neuregelung des Maßregelvollzugs berichtet. Im Nachgang hat er das Landeskrankenhaus in Uchtspringe besucht, um sich von der Einhaltung der datenschutzrechtlichen Rahmenbedingungen zu überzeugen. Anhaltspunkte für erhebliche Bedenken bestanden nicht, einzelne Hinweise zur Optimierung konnten jedoch gegeben werden.

Der Maßregelvollzug wird als öffentliche Aufgabe durch die zu 100 % vom Land getragene Salus gGmbH als Beliehene und damit als öffentliche Stelle wahrgenommen.

Sämtliche Beschäftigte einschließlich der Pflegekräfte sind auf der gesetzlichen Grundlage zu Verwaltungsvollzugsbeamten bestellt worden. Den verfassungsrechtlichen Vorgaben zur Wahrnehmung hoheitlicher Aufgaben durch öffentlich Bedienstete ist damit Rechnung getragen worden (vgl. BVerfG NJW 2012, 1563).

Die Betreuung des Datennetzes der Einrichtung wird von einem Dienstleister wahrgenommen. Die Ausgestaltung entspricht grundsätzlich den datenschutzrechtlichen Vorgaben.

Die Informationstechnologie wird durch eine Domäne für die gesamte Salus gGmbH mit einer zentralen Speicherung in Magdeburg geprägt. Die Außenstellen sind durch eine VPN-Leitung angebunden. Seitens der Salus gGmbH wurde erläutert, dass der Zugriff auf die Informationstechnologie mit Hilfe von Berechtigungen derart konzeptioniert ist, dass kein übergreifender Zugriff möglich ist. Medizinische Versorgungszentren sind nicht an das zentrale Krankenhausinformationssystem angeschlossen.

Die Dokumentation der Behandlung der Patienten im Maßregelvollzug erfolgt auf Papier. Lediglich die Grunddaten zum Patienten, die durch die gerichtlichen Entscheidungen eingehen, sind im zentralen System vermerkt.

Die allgemeine Anfertigung von Bildaufzeichnungen erfolgt auf der Grundlage von § 33 Abs. 1 MVollzG LSA. Auf den Stationen befinden sich Monitore, die die laufende Beobachtung auf der Station gestatten. Die Videoüberwachung wird dezentral vor Ort in Uchtspringe gespeichert. Die Löschung erfolgt automatisch durch Überspielen nach 48 Stunden.

Im Foyer hinter der zentralen Eingangsschleuse befinden sich einige Tische mit Stühlen für wartende Patienten und Besucher sowie Schließfächer für die Mitarbeiter. Der Raum wird an den vier Ecken durch drei herkömmliche und eine Dome-Kamera überwacht. Hierzu wurde im Rahmen der Beratung darauf hingewiesen, dass zunächst grundsätzlich die Erforderlichkeit des Einsatzes optisch-elektronischer Beobachtung zu dokumentieren ist. Zur Kontrolle von Zugangsberechtigungen besteht grundsätzlich ein Überwachungsanlass. Im Bereich mit Tischen und Stühlen für längeren Aufenthalt besteht aber ein stärkeres Interesse der Betroffenen,

nicht technisch beobachtet und aufgenommen zu werden; insoweit wurden Änderungen gefordert.

Nähere Einsicht gewährte der Besuch einer Station. Hier stand die Frage nach dem Einsatz von Videoüberwachungen insbesondere in Bezug auf schützenswerte Bereiche im Vordergrund. Die Bilder der Kameras zeigten zwei Monitore im Stationszimmer an. Die Aufnahmen wurden aufgezeichnet.

Hierzu wurde auf die differenzierte Regelung nach § 33 Abs. 2 MVollzG LSA hingewiesen. Danach ist zunächst der Einsatz technischer Mittel zur optisch-elektronischen Beobachtung möglich, wenn konkrete Anhaltspunkte der unmittelbaren Gefahr einer Selbsttötung oder einer erheblichen Selbstverletzung vorliegen. Schon dieser äußerst gravierende Eingriff in das Persönlichkeitsrecht der Betroffenen (dauerhafter Überwachungsdruck) bedurfte einer besonderen Begründung.

Die weitergehende Aufzeichnung ist nach § 33 Abs. 2 Satz 2 MVollzG LSA nur zulässig, wenn der Gefahr nicht anders begegnet werden kann. Diese noch gesteigerte Form des Grundrechtseingriffs bedarf einer entsprechend intensiveren Begründung im Einzelfall. Es wurde erläutert, dass eine pauschale Aufzeichnung rechtswidrig wäre. Unter Bezugnahme auf einen konkreten Vorgang wurde auch der Einsatz von Videoaufzeichnungen zu Therapiezwecken erörtert.

Auf der Station haben Pfleger Zugang zu Schränken mit den Patientenordnern. Neben differenzierten medizinischen und psychologischen Dokumentationen und Behandlungsplanung sind auch Verwaltungsvorgänge enthalten. Die Datennutzung ist zwar für den Vollzug der Unterbringung zulässig, jedoch nur „soweit dies erforderlich ist“. Dabei dürfte unzweifelhaft sein, dass für die Sicherstellung einer sachgerechten Pflege Grundkenntnisse über das Erkrankungsbild und seine Erscheinungsformen sowie über die vorgegebenen pflegerischen und therapeutischen Maßnahmen erforderlich sind. Die Notwendigkeit vollumfänglichen Zugriffs auf sämtliche medizinischen und therapeutischen Daten und insbesondere Verwaltungsdaten wurde aber hinterfragt. Dies gilt in besonderem Maße für Verwaltungsvorgänge wie beispielsweise Beschwerden an den Landesbeauftragten oder laufenden Schriftverkehr nach § 109 Strafvollzugsgesetz. Insoweit wurde die Prüfung und Reduzierung des Datenbestandes auf das für die Stationsarbeit Erforderliche angeregt.

Weitere datenschutzrelevante Aspekte, wie z. B. eine gesonderte Datei mit Informationen für eventuelle Fahndungen, die Protokollierung von Datenverarbeitungen, die Archivierung und der Umgang mit Besucherdaten wurden erörtert.

10.1.4 Landeskrebsregister

In Sachsen-Anhalt sollte die Vollständigkeit und Datenqualität der gemeldeten und dokumentierten Tumorerkrankungen zum Zweck der onkologischen Qualitätssicherung erhöht werden. Durch Langzeitbeobachtungen

würden Aussagen über die Qualität der Früherkennung, der Diagnostik und der Therapie möglich. Deshalb wurde angestrebt, neben den Auswertungen in den drei klinischen Registern im Land auch ein landesweites Register einzurichten, in dem (Teil-)Datenbestände zusammengeführt und Doppelmeldungen aussortiert werden können. Der Landesbeauftragte hatte bereits im X. Tätigkeitsbericht (Nr. 12.7) auf dieses Projekt hingewiesen. Es unterscheidet sich vor allem im Datenumfang von der bestehenden Registrierung auf staatsvertraglicher Grundlage zu Zwecken epidemiologischer Forschung im Gemeinsamen Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen.

In den Beratungen standen Fragen der technisch-organisatorischen Datensicherheit und der Gestaltung der Einwilligung der betroffenen Patienten im Vordergrund. Aufgebaut war das Verfahren auf der schon bisher erfolgenden Datenerhebung durch klinische Tumorregister. Von dort aus sollten die gesetzlich vorgegebenen Meldungen kleineren Umfangs an das epidemiologische Krebsregister, das Gemeinsame Krebsregister, übermittelt werden. Das Landeskrebsregister sollte aus Kostengründen an der Universität angegliedert sein. Die beiden anderen regionalen klinischen Register hätten angeschlossen werden können.

In den Beratungen konnte ein Konzept erarbeitet werden, das u. a. infolge des Einsatzes verschiedener Verschlüsselungsverfahren eine pseudonyme Datenhaltung im Landeskrebsregister gewährleisten würde. Dennoch wären die von den Forschern gewünschten Informationen aus dem Landeskrebsregister zu erlangen. Kumulierte Daten hätten sogar über das Internet allgemein zur Verfügung gestanden.

Schwierig war die kurze und verständliche Gestaltung der Einwilligungserklärung. Insgesamt konnte übereinstimmend ein dem Forschungsanliegen und dem Persönlichkeitsschutz der Patienten Rechnung tragendes Konzept erstellt werden. Ob und inwieweit dieses datenschutzfreundliche Konzept zur Umsetzung gelangen wird, ist aufgrund der bundesgesetzlichen Vorgaben zur Schaffung von Krebsregistern im Krebsfrüherkennungs- und Registergesetz offen (Gesetz vom 3. April 2013, BGBl. I S. 617).

Die neuen bundesrechtlichen Vorgaben formulieren Maßnahmen zur Verbesserung der Früherkennung von Krebserkrankungen. Weiter ist die Einführung flächendeckender klinischer Krebsregister durch die Länder vorgesehen. Mit dem Gesetz wird der Nationale Krebsplan umgesetzt. Der Landesbeauftragte wird die Entwicklung weiter begleiten.

Im Gemeinsamen Krebsregister werden Daten über individuelle Fälle von Krebserkrankungen für die epidemiologische Forschung mit Kontrollnummern pseudonymisiert gespeichert. Die Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten verwendet.

Die Verfahren zur Bildung der Kontrollnummern gewährleisten jedoch nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht mehr den erforderlichen Schutz dieser höchst sensiblen Daten. Daher haben sie mit der Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“ nebst Anforderungskatalog (**Anlage 23**) eine Überarbeitung der Kontrollnummern gefordert.

10.1.5 Herzinfarktregister Sachsen-Anhalt

Infolge der signifikant hohen Mortalitätsrate der Herz-Kreislauf-Erkrankungen in Sachsen-Anhalt beabsichtigten die Medizinischen Fakultäten der Universitäten in Kooperation ein Regionales Herzinfarktregister (RHESA) aufzubauen, um Erkenntnisse zum Vorhandensein von Risikofaktoren, zu strukturellen Voraussetzungen der Behandlung und zur Prozess-Qualität der Versorgung zu erhalten. Der Landesbeauftragte hatte Gelegenheit, mit datenschutzrechtlicher Beratung zum Projekt beizutragen.

Wesentliche Rechtsgrundlage für Datenerhebungen über Herzinfarktpatienten ist die Einwilligung. Daher stand aus datenschutzrechtlicher Sicht die Ausgestaltung der Patienteninformation und der Einwilligungserklärung im Vordergrund. Für die Patienteninformation ist zu berücksichtigen, dass nicht mehr Daten erhoben werden dürfen als erforderlich und dass der Patient erkennen können muss, worin er einwilligt. So wurde erläutert, dass die Befugnis der Handelnden (Krankenhausarzt, Hausarzt, Rettungsdienst usw.) zur Informationsübermittlung deutlich sein müsse. Für jeden Handelnden müsse in dem jeweils gewünschten Umfang eine Einwilligung als datenschutzrechtliche Übermittlungsbefugnis sowie ggf. eine Entbindung von der berufsrechtlichen Schweigepflicht vorliegen. Zudem war auf die präzise Darstellung der vorgesehenen Verwendung der Daten hinzuweisen, damit ersichtlich wird, wer in welchem Umfang auf welche Daten (medizinische, personenbezogene) zugreift. Auch der Umfang der im Einzelfall vom jeweils Handelnden zu übermittelnden Daten sollte ebenfalls deutlich beschrieben sein. Da auch Abfragen beim Hausarzt vorgesehen waren, schien eine Differenzierung geboten. Langjährig zurückliegende Behandlungen zu Beschwerden oder Erkrankungen ohne Auswirkung auf einen späteren Infarkt sollten ausdrücklich von der Einwilligung ausgenommen sein.

Weiter wurden gegen eine unbegrenzte Speicherung Bedenken erhoben. Eine unendliche Speicherung schien mit den verfassungsrechtlichen Geboten der Erforderlichkeit und Verhältnismäßigkeit nicht vereinbar. Auch wurde die datenschutzkonforme Löschung von Patientendaten angesprochen.

Im Fall des Versterbens sollte der leichenschauende Arzt neben der Todesbescheinigung einen Todesfallerhebungsbogen ausfüllen und an das Gesundheitsamt senden. Dieses sollte auf den Unterlagen Pseudonyme vermerken und ohne Personenbezug an das Register senden. Dem standen im Hinblick auf § 1 Abs. 5 Satz 1 Bestattungsverordnung Sachsen-Anhalt nur bezüglich der Todesbescheinigung keine Bedenken entgegen.

Problematisch war dagegen die Absicht, das Gesundheitsamt um personenbezogene Recherche bei weiteren Ärzten (u. a. Hausarzt) zu bitten. Eine Offenbarungsbefugnis, die nach § 203 StGB geboten gewesen wäre, war nicht ohne Weiteres ersichtlich. Mit dem Instrument einer mutmaßlichen Einwilligung des Verstorbenen zu arbeiten (zu einem ähnlichen Fall vgl. Bundesgerichtshof, Urteil vom 26. Februar 2013, NZS 2013, 553), würde dem jeweiligen Arzt die Pflicht auflegen, im Einzelfall das Vorliegen der rechtlichen Voraussetzungen zu prüfen.

Demgemäß wurde empfohlen, ein Verfahren zu wählen, bei dem die Offenbarung personenbezogener Daten unterbleibt. So kann das Gesundheitsamt, dem die Ärzte über die Todesbescheinigung bekannt sind, vorgefertigte Umschläge an die Ärzte versenden. Werden die Umschläge an das Register adressiert und nur die Pseudonyme darauf vermerkt (Sterbebuchnummer), kann der Arzt die gewünschten Bögen ohne Personenbezug ausfüllen und versenden. Das Register kann die Unterlagen über das Pseudonym dennoch einem (unbenannten) Individuum zuordnen.

10.1.6 Krankenhausentlassungsberichte

Die Anforderung von Krankenhausentlassungsberichten durch die Krankenkasse zu Zwecken des Krankengeldfallmanagements wurde im Berichtszeitraum wieder zunehmend thematisiert. Sie ist umfänglich im Kreise der Datenschutzbeauftragten des Bundes und der Länder angesprochen worden. Auch Eingaben von Ärzten und Einrichtungen wiesen auf die Problematik hin.

Das Themengebiet umschreibt eine äußerst komplexe rechtliche Problematik, bei der vielfältige Vorschriften zusammenwirken und im erheblichen Maß konkrete Umstände des Einzelfalles zu berücksichtigen sind.

Regelungen zu zulässigen Datenerhebungen durch Krankenkassen finden sich in § 284 Abs. 1 SGB V. Korrespondierend ist nach § 100 SGB X vorgesehen, dass Ärzte verpflichtet sind, den Leistungsträgern im Einzelfall auf Verlangen Auskunft zu erteilen, soweit das für die Durchführung von deren Aufgaben nach dem SGB erforderlich ist und es gesetzlich zugelassen ist oder der Betroffene im Einzelfall eingewilligt hat. Dabei ist die Auskunftspflicht sicherlich nicht völlig umfassend, sondern bedarf eines konkretisierenden Verlangens des Leistungsträgers. Inhalt der Mitwirkungspflicht ist das Erteilen von Auskünften, nicht notwendig die Vorlage von Unterlagen.

10.1.7 GKV-Versorgungsstrukturgesetz

Mit dem „Gesetz zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung“ vom 22. Dezember 2011 (BGBl. I S. 2983) soll dem Ärztemangel in ländlichen Regionen begegnet werden. Das Gesetz enthält auch datenschutzrechtliche Regelungen. Unter anderem sind Vorschriften zur Datentransparenz im SGB V (§§ 303a bis 303e SGB V) betroffen. Danach dürfen Daten des Informationssystems der gesetzlichen Krankenversicherung (Arbeitsgemeinschaft für Aufgaben der

Datentransparenz mit Vertrauensstelle und Datenaufbereitungsstelle) mit anonymisierten Versorgungsdaten der gesetzlichen Krankenkassen insbesondere für Zwecke der Versorgungsforschung und für Steuerungsaufgaben in der gesetzlichen Krankenversicherung von den in § 303e SGB V genannten Einrichtungen zur Erfüllung ihrer Aufgaben verarbeitet und genutzt werden. Die Daten werden lediglich anonymisiert zur Verfügung gestellt. Das Nähere regelt die Datentransparenzverordnung vom 10. September 2012 (BGBl. I S. 1895).

Ergänzt wurde auch die Regelung des § 197a SGB V zu Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen. Hierzu hatte der Landesbeauftragte im VIII. Tätigkeitsbericht (Nr. 20.12) darauf hingewiesen, dass nach alter Rechtslage keine Übermittlungen möglich sind. Nunmehr können nach dem neuen Abs. 3a Übermittlungen im Rahmen der Zusammenarbeit der Einrichtungen zur Bekämpfung von Fehlverhalten bei Krankenkassen und Kassenärztlichen Vereinigungen stattfinden.

10.1.8 Patientenrechtegesetz

Am 26. Februar 2013 ist das Gesetz zur Verbesserung der Rechte von Patienten (BGBl. I S. 277) in Kraft getreten. Das Gesetz kodifiziert u. a. die bisherigen richterrechtlichen Grundsätze des Arzthaftungs- und Behandlungsrechts im Bürgerlichen Gesetzbuch (BGB) in einem neuen Untertitel „Behandlungsvertrag“ (§§ 630a bis 630h). Die neuen Regelungen betreffen Informations- und Aufklärungspflichten des Arztes, die Pflicht zur Dokumentation der Behandlung und das Akteneinsichtsrecht der Patienten sowie die Grundzüge der Beweislast bei Fehlern.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich eingehend mit der Problematik befasst und umfängliche Verbesserungsempfehlungen zum Referentenentwurf übersandt. Die Konferenz hat am 23. Mai 2012 die Entschließung „Patientenrechte müssen umfassend gestärkt werden“ gefasst (**Anlage 13**).

Unter anderem ging es darum, dass Patienten nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden dürfen, die keinen Behandlungsbezug haben. Die Patienten sollten hinreichend auch über Behandlungsfehler informiert werden, die Auskunfts- und Akteneinsichtsrechte sollten verfassungskonform klar geregelt und die Aspekte der Archivierung und Löschung bedacht werden. Weiter schienen Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) sinnvoll.

Leider sind die Empfehlungen der Datenschutzbeauftragten nur sehr unvollkommen berücksichtigt worden.

10.1.9 Langfristige Aufbewahrung von Patientenakten

Von einem Universitätsklinikum wurde die Frage aufgeworfen, ob man nicht die Akten stationärer Patienten über 30 Jahre nach der Behandlung hinaus aufbewahren dürfe. Die Unterlagen könnten der Forschung dienen.

Dafür sprächen das Forschungsprivileg und die Wissenschaftsfreiheit. Das Vorhaben der Aktenaufbewahrung von bis zu 30 Jahren wird häufig mit dem Hinweis auf die Verjährungsvorschrift des § 199 BGB begründet.

Die Aufbewahrung von Patientenakten stellt eine Speicherung und damit eine Datenverarbeitung dar. Dies bedarf einer rechtlichen Grundlage in Gestalt der Einwilligung des Betroffenen bzw. einer gesetzlichen Regelung (§ 3 Abs. 2 Nr. 1 DSG LSA i. V. m. § 4 Abs. 1 BDSG).

Eine allgemeine Vorschrift zur langfristigen Aufbewahrung von Akten stationärer Patienten ist nicht ersichtlich. Lediglich für bestimmte fachliche Bereiche wird in Spezialvorschriften eine Aufbewahrungszeit von Patientenunterlagen vorgegeben (z. B. Betäubungsmittelverschreibungsverordnung, Strahlenschutzverordnung, Röntgenverordnung usw.). Sonst gilt der Grundsatz, dass personenbezogene Informationen dann zu löschen sind, wenn sie für die Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich sind (§ 20 Abs. 2 Nr. 2 BDSG). Ausdrückliche informierte Einwilligungen dürften zumeist nicht vorliegen. Auch von einem mit dem Abschluss des Behandlungsvertrages erklärten allgemeinen Einverständnis des Patienten in eine Aufbewahrung seiner Unterlagen für einen derart langen Zeitraum jenseits spezifischer Notwendigkeiten kann nicht ausgegangen werden.

Der Hinweis auf eine rechtlich theoretische Möglichkeit der Haftung vermag nicht die Erforderlichkeit im datenschutzrechtlichen Sinn für den regelmäßigen Bedarf zur Abwicklung von Verwaltungsaufgaben zu begründen. Zweifellos besteht ein berechtigtes Interesse der Klinikverwaltung, Unterlagen für die Abwehr zu erwartender Schadenersatzansprüche aufzubewahren. Auf der anderen Seite sind auch die Persönlichkeitsrechte der betroffenen Patienten zu berücksichtigen. Demgemäß dürfte es lediglich in Einzelfällen bzw. in Bezug auf bestimmte Erkrankungsarten (z. B. chronisch Kranke) anzunehmen sein, dass hier auch nach Jahrzehnten noch mit der Geltendmachung von Ansprüchen zu rechnen ist. Gegebenenfalls können auch einzelne komplizierte Behandlungsvorgänge mit äußerst hohem Schadenspotential in die Betrachtung einbezogen werden.

Die allgemeine Notwendigkeit einer dreißigjährigen Speicherung von Patientendaten wird jedoch auch in Fachkreisen zumeist nicht gesehen. So gibt es viele Einrichtungen, die schon aus Gründen kostenintensiver Speicherung und Aktenaufbewahrung die Vorgänge grundsätzlich nach zehn Jahren vernichten, soweit nicht im Einzelfall Ausnahmegründe vorliegen. Auch die Orientierungshilfe zu Krankenhausinformationssystemen (abrufbar auf der Homepage des Landesbeauftragten) gibt eine möglichst frühzeitige Löschung vor. Die Empfehlungen der Bundesärztekammer zur ärztlichen Schweigepflicht verweisen zur Aufbewahrungsfrist auf eine individuelle realistische Einschätzung in medizinischer Sicht. Auch § 10 Abs. 3 der Musterberufsordnung der Ärztekammer Sachsen-Anhalt geht grundsätzlich von einer Aufbewahrungszeit von zehn Jahren aus, unter Berücksichtigung der berufsständischen Einschätzung der Erforderlichkeit der Dokumentation. Auch dürfte haftungsrechtlich Folgendes gelten: Braucht der Arzt oder Krankenhausträger die Krankenunterlagen nicht

länger aufzubewahren, darf ihm wegen deren Vernichtung oder wegen eines Verlustes hieraus kein Nachteil mehr entstehen (Oberlandesgericht Hamm, Urteil vom 29. Januar 2003, Az.: 3 U 91/02, Versicherungsrecht 2005, 412). Soweit noch Bedenken bestehen, könnte die Problematik mit dem Haftpflichtversicherer erörtert werden.

Informationen über die Gesundheit von Patienten stellen sicher eine gesellschaftliche Ressource dar, die für die Forschung von Wert ist. Demgemäß gibt es auch vielfache internationale Diskussionen über das Verhältnis der Patientenrechte und wissenschaftlichen Verwendungszwecken. Zumeist wird auf die Notwendigkeit von Einwilligungen verwiesen, da es sich um sensible Informationen handele, die nach internationalen Grundsätzen geschützt sind.

In anderen Ländern gibt es teilweise spezielle gesetzliche Vorschriften, die die Nutzung von Daten zulassen, wenn das öffentliche Interesse an Forschungsvorhaben das schützenswerte Interesse der Patienten überwiegt. Eine derartige spezielle Rechtsgrundlage für die Datenverarbeitung bzw. -nutzung existiert in Sachsen-Anhalt nicht. Die hochschulrechtlichen Regelungen des Landes gewähren nur Unterstützung und Zusammenarbeit zwischen Klinikum und Forschern in konzeptioneller und organisatorischer Hinsicht. Eine Rechtsgrundlage zur Datenverarbeitung ist den Aufgaben und Strukturvorgaben nicht zu entnehmen. Auch die Regelung des Forschungsprivilegs nach § 28 Abs. 6 Nr. 4, Abs. 8 Satz 1 BDSG ist hier keine Rechtsgrundlage. Es wäre jeweils eine konkrete Abwägung im Einzelfall geboten. Die beabsichtigte pauschale Aufbewahrung hätte letztlich im Hinblick auf zunächst noch nicht bestimmte Forschungsprojekte eine Vorratsdatenspeicherung bedeutet. Auch das Grundrecht der Wissenschaftsfreiheit aus Art. 5 Abs. 3 Satz 1 GG vermittelte letztlich keine drittbezogenen Ansprüche. Daher musste von der angedachten langfristigen Speicherung abgeraten werden.

10.1.10 Abrechnungsberater für Ärzte

Ein Nachrichtenmagazin berichtete von einem Sachverständigen in Sachsen-Anhalt, der von Ärzten patientenbezogene Daten auf einem USB-Stick erhalte zum Zweck der Beratung über die Abrechnung bzw. die Optimierung der Verordnungen. Damit könnten Strafzahlungen vermieden werden, wenn Ärzte im Vergleich zu anderen unverhältnismäßig viel verschreiben. Pharmareferenten würden Ärzten dies nahelegen.

Die Rechtsgrundlagen eines derartigen Verfahrens waren fraglich. Nötig wäre eine Offenbarungsbefugnis in Bezug auf die ärztliche Schweigepflicht. Ein selbständiger, auf akademischem Niveau handelnder Sachverständiger ist anders als etwa die Sprechstundenhilfe kein berufsmäßiger Gehilfe des Arztes, der ohne weitere Grundlage Kenntnis erlangen darf. Zudem müssten die Datenerhebungs- und Verarbeitungsbefugnisse des BDSG dem Sachverständigen den Umgang mit den zumindest wohl personenbeziehbaren Patientendaten gestatten.

Der Sachverständige hat dem Landesbeauftragten mitgeteilt, er würde die anfragenden Ärzte individuell beraten und keine Daten an Dritte herausgeben. Die Namen der Patienten könnte er zudem auch nicht unmittelbar sehen. Er habe das Verfahren vor dem Hintergrund der öffentlichen Diskussion zunächst eingestellt.

Der Landesbeauftragte hielt das Verfahren nach einer vorläufigen Bewertung hinsichtlich der Offenbarungsbefugnisse der Ärzte und der Verarbeitungsbefugnisse des Sachverständigen für kritisch. Die Ärztekammer Sachsen-Anhalt wurde darauf hingewiesen und hat die Thematik zur Sensibilisierung der Ärzte veröffentlicht. Dem Sachverständigen wurde empfohlen, das Verfahren dahin zu verändern, dass kein Personenbezug des Datenbestandes mehr gegeben ist. Da der Landesbeauftragte nicht ausschließen konnte, dass ggf. ein strafbares Vorgehen vorlag, war er aus prozessualen Gründen gehalten, das Verfahren an die Staatsanwaltschaft abzugeben.

10.1.11 Rettungsdienstprotokolle im Personalamt

In einem Landkreis wurden auf Anforderung der Personalamtsleiterin und in Abstimmung mit dem Ordnungsamtsdezernenten zum Zweck der Bewertung der Auslastung des Leitstellenpersonals sämtliche Einsatzprotokolle der Leitstelle eines Monats dem Personalamt zur Verfügung gestellt. Die Protokolle wiesen sensible Patientendaten, wie z. B. Name, Anschrift, Grund des Einsatzes, Art der Verletzung und Diagnoseschlüssel, aus.

Bereits als die behördliche Datenschutzbeauftragte davon Kenntnis erlangte, wurde das Verfahren eingestellt und die Einsatzprotokolle wurden an die Leitstelle zurückgegeben.

Darüber hinaus hatte der Landesbeauftragte den Landkreis ausführlich darüber aufgeklärt, dass es sich bei diesem Vorgang um eine personenbezogene Datennutzung nach § 2 Abs. 6 DSG LSA handelte, die einer Rechtsgrundlage bedurfte. Allerdings waren weder die Voraussetzungen des § 14 Abs. 1 Rettungsdienstgesetz Sachsen-Anhalt (RettDG LSA) a. F. noch die des § 26 DSG LSA erfüllt. Darüber hinaus handelte es sich bei diesen Daten um Patientendaten, die zusätzlich der ärztlichen Schweigepflicht nach § 203 Strafgesetzbuch unterlagen. Eine Befugnis zur Durchbrechung der Schweigepflicht schien ebenfalls nicht gegeben. Auch nach der Neufassung des Rettungsdienstgesetzes (vgl. Nr. 10.1.12) stehen dem Träger des Rettungsdienstes für Planungs- und Bewertungszwecke nur anonymisierte Protokollfassungen zu (§ 20 Abs. 6 RettDG LSA).

10.1.12 Rettungsdienstgesetz

Mit dem Entwurf eines Gesetzes zur Neuregelung des Rettungswesens war der Landesbeauftragte zunächst nicht befasst, da die Landesregierung ihn bei der Erarbeitung entgegen § 14 Abs. 1 Satz 3 DSG LSA nicht beteiligt hatte. Angesichts der Aufzählung vieler Vorschriften des Gesetzentwurfs (LT-Drs. 6/1255) in Artikel 1 § 50, die jeweils zu einer Einschränkung von Datenschutzgrundrechten führen, war eine Beteiligung aber an-

gezeigt. Der Ausschuss für Inneres und Sport des Landtages von Sachsen-Anhalt gab dem Landesbeauftragten dann Gelegenheit zur Stellungnahme.

In vielen Punkten bestanden keine Bedenken. Neben redaktionellen Hinweisen konnte jedoch auf einige Unstimmigkeiten hingewiesen werden.

Der Entwurf behielt die Aufbewahrung von Aufzeichnungen und Protokollen stets für zwölf Monate bei (vgl. hierzu VIII. Tätigkeitsbericht, Nr. 10.6). Ob der seinerzeit angenommene Bedarf, Daten länger als drei bzw. sechs Monate zu speichern, Bestätigung gefunden hat, war nicht dokumentiert.

Vor allem in Protokollen zur Patientenübergabe sind wohl viele medizinische Daten enthalten, zu deren Interpretation die Verwaltung der Leistungsträger mangels medizinischer Kompetenzen zunächst kaum in der Lage sein dürfte.

Einer der weiteren Problemkreise ist das teilweise erhebliche Interesse von Krankenkassen an medizinischen Daten im Zusammenhang mit der Abrechnung bzw. Überprüfung von Rettungsdienstleistungen. Zur Anpassung des Dokumentationsverfahrens an die sozialversicherungsrechtlichen Vorgaben enthält das Gesetz keine Hinweise, im Rahmen einer vorgesehenen Verordnung kann dem aber wohl Rechnung getragen werden.

Das Gesetz ist am 1. Januar 2013 in Kraft getreten (GVBl. LSA 2012 S. 624).

10.1.13 Software im Gesundheitsamt

Auch in diesem Berichtszeitraum (vgl. X. Tätigkeitsbericht, Nr. 12.3) hat der Landesbeauftragte das Gesundheitsamt eines Landkreises aufgesucht, um die Datenerhebung und -verarbeitung bei Einschulungsuntersuchungen und schulärztlichen Untersuchungen zu prüfen. Diesmal lag der Schwerpunkt der datenschutzrechtlichen Kontrolle bei der landesweit zu verwendenden Software Octoware.

Diesbezüglich wurden zwei gravierende datenschutzrechtliche Probleme festgestellt. Hierbei handelt es sich um das Archivieren bzw. Löschen nicht mehr benötigter personenbezogener Daten und um den Zugriff auf die sog. Zentralkartei.

Da die Akten der untersuchten Kinder ab deren 18. Lebensjahr für zehn Jahre im Verwaltungsarchiv des Landkreises aufbewahrt und danach vernichtet werden, müsste diese Verfahrensweise auch in Octoware abgebildet werden. Das heißt, die Daten müssten automatisch zum Stichtag 18. Geburtstag archiviert werden und ein Zugriff auf diese Daten dürfte nicht mehr oder nur für einen stark eingeschränkten Personenkreis möglich sein, der das Recht besitzt, im Einzelfall archivierte Daten zu reaktivieren. Außerdem müsste nach zehn Jahren eine automatische Löschung der Daten erfolgen.

Diese Funktionen sind in Octoware nicht vorhanden. Die Daten können zwar zum Stichtag 18. Geburtstag automatisch als archiviert gekennzeichnet werden, aber der Zugriff auf diese Daten bleibt weiterhin möglich. Eine automatische Löschung der Daten erfolgt ebenfalls nicht, manuelles Löschen wäre mit hohem Zeitaufwand möglich.

Ein weiteres Problem ist der Zugriff auf die sog. Zentralkartei, der wohl von allen Modulen aus uneingeschränkt möglich ist. Das hat zur Folge, dass auch Mitarbeiter des Kinder- und Jugendärztlichen Dienstes auf Patientendaten zugreifen können, die sie zu ihrer Aufgabenerfüllung nicht benötigen. Außerdem ist davon auszugehen, dass Mitarbeiter anderer Bereiche des Gesundheitsamtes, die andere Octoware-Module nutzen, ebenfalls Zugriff auf die Daten aller Kinder haben, die im Kinder- und Jugendärztlichen Dienst untersucht wurden.

Aufgrund der Vermutung, dass es sich nicht um landkreisspezifische Probleme handelt, sondern diese vielmehr in der Software begründet sind, wurde ein weiteres Gesundheitsamt dahingehend kontrolliert. Im Ergebnis mussten dieselben datenschutzrechtlichen Problemlagen festgestellt werden.

Daraufhin wurde versucht, mit dem Hersteller der Software die geschilderten Probleme zu klären. Dieser teilte mit, dass für die Bereiche Jugendärztlicher Dienst und Jugendzahnärztlicher Dienst noch keine Löschroutinen zur Verfügung stünden. Allerdings wurde ein Programm-Update für 2012 in Aussicht gestellt. Ob dieses Update bereits erfolgt ist, konnte trotz Nachfrage bisher nicht geklärt werden. Zu der Frage des scheinbar uneingeschränkten Zugriffs auf die Zentralkartei (z. B. haben Mitarbeiter des Kinder- und Jugendärztlichen Dienstes auch Zugriff auf Daten älterer Patienten (Geburtsjahr 1950), die von einem niedergelassenen Arzt gemeldete Impfungen enthalten), wurde erklärt, dass Ärzte im Jugendärztlichen Dienst auch Schutzimpfungen gem. § 4 des Gesundheitsdienstgesetzes Sachsen-Anhalt unabhängig vom Alter durchführen können, sodass aus diesem Grund ein Zugriff auf diese Daten notwendig sei.

Diese Auffassung kann nicht geteilt werden, da mit dem Octoware-Modul „Schutzimpfungen“ die Möglichkeit der getrennten Erfassung dieser Daten besteht und der Arzt bei der Durchführung einer solchen Impfung aus dem Modul „Jugendärztlicher Dienst“ in das Modul „Schutzimpfungen“ wechseln kann. So wäre sichergestellt, dass der jeweilige Nutzer im jeweiligen Modul nur Zugriff auf die Daten erhält, die für seine Aufgabenerfüllung notwendig sind. Dass Mitarbeiter, die mehrere Module nutzen, zwangsläufig Zugriff auf größere Datenmengen haben, ist dabei unerheblich. Wichtig ist, dass auch innerhalb einer verantwortlichen Stelle wie dem Gesundheitsamt eine aufgabenspezifische Trennung im Umgang mit personenbezogenen Daten erfolgt (informationelle Gewaltenteilung). Da nicht jeder Mitarbeiter des Gesundheitsamtes Zugriff auf alle Papierakten hat und haben muss, darf auch nicht jeder Mitarbeiter Zugriff auf alle personenbezogenen Daten in der Zentralkartei erhalten.

Zusammenfassend ist festzustellen, dass trotz der erheblichen datenschutzrechtlichen Bedenken weder der Landkreis noch der Softwarehersteller konkrete Maßnahmen mitgeteilt haben, die o. g. Verfahren datenschutzgerecht zu gestalten. Mittlerweile hat der Landesbeauftragte das Landesamt für Verbraucherschutz entsprechend informiert, da dieses für die Standardisierung der Einschulungsuntersuchung zuständig ist.

10.1.14 Dopingbekämpfung

Die Bekämpfung des Dopings im nationalen wie internationalen Leistungssport ist ein hehres Ziel, dem auch der Landesbeauftragte grundsätzlich nicht im Wege stehen will. Sie darf aber nicht dazu führen, dass für die betroffenen Athleten, die sich dem nationalen Anti-Doping-Code unterwerfen müssen, um überhaupt an Wettbewerben teilnehmen zu können, quasi die Grundrechte nicht mehr gelten und sie als gläserne Sportler gedemütigt werden.

Es muss z. B. sichergestellt werden, dass notwendige Kontrollen nicht in der Weise geschehen, dass die Menschenwürde beeinträchtigt ist. Problematisch erscheinen hier insbesondere Sichtkontrollen bei der Abgabe von Urinproben, Aufenthalts- und Bewegungsprofile infolge eines rigiden Meldesystems und die Übermittlung personenbezogener Daten an die WADA (Welt-Anti-Doping-Agentur), und das alles auf der zweifelhaften Rechtsgrundlage einer Einwilligung. Die Datenübermittlung muss nach Ansicht des Landesbeauftragten auf Einzelfälle beschränkt werden, z. B. bei Kontrollen im Ausland. Bei der Datenübermittlung in Staaten ohne angemessenes Datenschutzniveau müssen Vorkehrungen getroffen werden, sodass die Athleten sicher sein können, dass ihre Daten nach EU-Standards behandelt werden.

Deshalb versuchen die Datenschutzaufsichtsbehörden, insbesondere der Landesbeauftragte von Nordrhein-Westfalen, schon seit Jahren, mit der Nationalen Anti-Doping-Agentur (NADA), dem Bundesministerium des Innern, dem Deutschen Olympischen Sportbund und den Sportverbänden ins Gespräch zu kommen. Gebracht hat das bisher nicht viel, auch weil die NADA an die Vorgaben der internationalen Dopingagentur WADA gebunden ist. Immerhin hat man inzwischen bei der NADA einen Ombudsmann installiert, an den sich Sportler wenden können, und ein Beschwerdeverfahren eingerichtet. Auch ein Datenschutzbeauftragter wurde bestellt. Mittlerweile dürfen Minderjährige, die das 16. Lebensjahr noch nicht vollendet haben, die Beobachtung bei der Urinprobe ablehnen.

Aktuelle Dopingfälle und eine vom Bundesinstitut für Sportwissenschaft begleitete Studie von Universitäten aus Münster und Berlin (veröffentlicht im August 2013) haben inzwischen dazu geführt, dass über ein Anti-Doping-Gesetz diskutiert wird (vornehmlich über die Bestrafung der Sportler selbst), in dem auch der Datenschutz geregelt werden könnte. Unabhängig davon wollen die Aufsichtsbehörden in weiteren Gesprächen datenschutzrechtliche Verbesserungen erreichen und so mittelbar auf den internationalen WADA-Code Einfluss nehmen.

10.2 Sozialwesen

10.2.1 Kontoauszüge in SGB II-Verfahren

Immer wieder erreichen den Landesbeauftragten Anfragen und Eingaben zur Anforderung von Kontoauszügen durch die Jobcenter. Vielfach bestehen bei den Antragstellern grundlegende Bedenken, oft werden auch konkrete Fragen zu Schwärzungen, beispielsweise in Bezug auf Kunden von selbständigen Leistungsempfängern, formuliert. Bereits im VIII. Tätigkeitsbericht (Nr. 20.2) und im IX. Tätigkeitsbericht (Nr. 21.3) hat sich der Landesbeauftragte ausführlich mit der Problematik beschäftigt. Weiter gibt es auf der Homepage „Gemeinsame Hinweise mehrerer Landesbeauftragter zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen“. Im jeweiligen Einzelfall ist zumeist die Abstimmung zwischen Leistungsträger und Leistungsempfänger nötig, um zu klären, welche Informationen der Leistungsträger abfragen kann und welche vom Leistungsempfänger durch Schwärzung unkenntlich gemacht werden können. Dabei wird nicht hinreichend beachtet, dass die Anforderung zur Einsicht – ggf. mit möglichen Schwärzungen – eher unproblematisch, die Speicherung von Kopien in den Akten dagegen zumeist unzulässig ist.

Im Formular „Vorzulegende Unterlagen bei Abgabe des Antrages“ wurde in einem Jobcenter, wie in wiederholter Prüfung festgestellt wurde, pauschal angekreuzt und dem Antragsteller vorgegeben, die „regelmäßig benötigten“ Unterlagen beizubringen. Dass dabei oft und trotz Hinweis des Landesbeauftragten „großzügig“ statt nach der Erforderlichkeit verfahren wird, ist bedenklich. Ohne nähere Beratung werden zudem zu Hause oft Angaben in Anträge eingetragen, die nicht erforderlich sind und deren Speicherung damit unzulässig wäre.

Nach dem Eindruck aus den Beratungen lassen es die Leistungsträger häufig an der gebotenen Sorgfalt bei der Anforderung mangeln. Die Begrenzung der Anforderung auf das zulässige Maß, das Unerlässliche, und die rechtzeitige Erörterung würden vielfach Unstimmigkeiten entgegen wirken. Fragen der Schwärzung könnten geklärt und die tatsächlichen Erforderlichkeiten erläutert werden.

10.2.2 Kopie des Personalausweises

Ein beliebtes Verfahren der Jobcenter ist das Kopieren des Personalausweises für die Akte. Zu dieser Praxis hatte sich der Landesbeauftragte bereits im VII. Tätigkeitsbericht (Nr. 20.4) geäußert. Das Grundrecht auf informationelle Selbstbestimmung und das Recht am eigenen Bild sind betroffen. Die Prüfung der Identität ist zwar nötig, die Speicherung der Kopien mit unnötigen Zusatzdaten ist jedoch nicht von den gesetzlichen Grundlagen gedeckt. Diesen Eindruck aber vermitteln die Behörden, die eine Kopie für die Akte ohne Weiteres einfordern bzw. anfertigen. In Beratungen mit einem Jobcenter wurde der Landesbeauftragte darauf aufmerksam gemacht, dass eine solche Kopie aber den Vorteil habe, dass auch Vertreter in der Sachbearbeitung die Identität anhand der Akte er-

kennen können, wenn spontane Leistungen beantragt werden. Hätte der Antragsteller den Ausweis nicht dabei, müsste er nach Hause geschickt werden. Die Kopie wäre also nicht zwingend erforderlich, aber nützlich. Demgemäß wurde mit dem Leistungsträger vereinbart, die Kopie auf der Grundlage der – informierten und zweckgebundenen – Einwilligung (zu den Voraussetzungen vgl. § 67b Abs. 2 SGB X) zu speichern.

10.2.3 Hausbesuche des Jobcenters

Die Durchführung von Hausbesuchen im Sozialwesen war bereits mehrfach Gegenstand der Tätigkeitsberichte des Landesbeauftragten für den Datenschutz (VI. Tätigkeitsbericht Nr. 20.4; X. Tätigkeitsbericht Nr. 22.3). Des Weiteren hat die Bundesagentur für Arbeit ihre „Fachlichen Hinweise zu § 6 SGB II“ überarbeitet und mit Handlungsempfehlung/Geschäftsanweisung (HEGA) 08/2010 veröffentlicht. Diese fachlichen Hinweise sind auf den Internetseiten der Bundesagentur für Arbeit veröffentlicht und bieten neben der Erläuterung der gesetzlichen Grundlagen weitere Orientierungen in Bezug auf Prüfauftrag, Ermittlungsauftrag, Prüfbericht sowie Protokoll. In Beratungen wird auf die besondere Sorgfalt bei der Anwendung dieses starken Eingriffsinstruments hingewiesen.

10.2.4 Räumliche Situation in Jobcentern

Auf die wegen möglichen Mithörens Unbefugter problematische räumliche Situation eines Jobcenters war dieses schon aufgrund einer Prüfung im Jahr 2008 hingewiesen worden. Leider hatte sich seitdem bis zur neuerlichen Prüfung 2011 nichts geändert. Als Minimum wurde nun gefordert, in allen Fluren auf offenbar schon vorhandene abgetrennte Räume („Anhörungszimmer“) deutlich aufmerksam zu machen und so den Betroffenen die Möglichkeit zu geben, selbst auf die Einhaltung der gesetzlichen Verpflichtung der Jobcenter zur Wahrung des Sozialgeheimnisses hinzuwirken.

Die Wahrung des Sozialgeheimnisses ist eine bundesgesetzliche Verpflichtung, gegen die man nicht jahrelang mit dem Hinweis verstoßen darf, man habe gerade nicht genug Räumlichkeiten.

10.2.5 Kinderschutz

Das Gesetz zur Kooperation und Information im Kinderschutz vom 22. Dezember 2011 (BGBl. I S. 2975; sog. Bundeskinderschutzgesetz) bezweckt, das Wohl von Kindern und Jugendlichen zu schützen und weiter zu fördern. Dazu gehört u. a., zu den in der Kinder- und Jugendhilfe Tätigen erweiterte Führungszeugnisse anzufordern und besser interdisziplinär zusammenzuarbeiten. Auch wurden die nach Landesrecht für die Information der Eltern zuständigen Stellen befugt, den Eltern ein persönliches Gespräch anzubieten, auf Wunsch der Eltern auch in ihrer Wohnung. Auch wenn hierbei die „häuslichen Verhältnisse“ wahrgenommen werden, bestehen gegen Beratungen datenschutzrechtlich keine Bedenken, wenn zuvor eine umfassende Aufklärung erfolgte und die Freiwilligkeit vollständig gewahrt ist.

Darüber hinaus hat auf Landesebene das „Zentrum Frühe Hilfen für Familien“ ein datenschutzgerechtes landeseinheitliches Verfahren zum Einsatz von Familienhebammen entwickelt, mit dem die Verpflichtungen der Familienhebammen und die berechtigten Interessen der bei den Jugendämtern eingerichteten „Lokalen Koordinierungsstellen Familienhebammen“ bedient werden können. Die Familienhebammen, die der ärztlichen Schweigepflicht nach § 203 Strafgesetzbuch unterliegen, können entweder von den Jugendämtern beauftragt werden oder Schwangere/Mütter wenden sich direkt an diese. Abgerechnet werden die erbrachten Leistungen in beiden Konstellationen bei den „Lokalen Koordinierungsstellen Familienhebammen“. Für die Fälle, dass sich Schwangere/Mütter direkt an die Familienhebammen wenden und keine Schweigepflichtentbindung zur personenbezogenen Datenübermittlung an die „Lokalen Koordinierungsstellen Familienhebammen“ erteilen, ist nunmehr ein pseudonymisiertes Übermittlungsverfahren vorgesehen.

11 Personalwesen

11.1 Personalvermittlungsstelle

Im Herbst 2012 erging der Beschluss der Landesregierung, eine Personalvermittlungsstelle (PVS) beim Ministerium der Finanzen einzurichten. Sie soll der ressortübergreifenden Vermittlung von Überhangpersonal dienen und Planpersonal unterstützen, das eine andere Verwendung anstrebt. Hierfür sollen die Ressorts mittels eines Vordrucks Personalprofile an die PVS melden.

Die Problematik der ressortübergreifenden Übermittlung von Personalaktendaten durch personalaktenführende Dienststellen ist mit dem seinerzeit zuständigen Ministerium seit Jahren intensiv erörtert worden. Dabei wurde durch den Landesbeauftragten immer wieder darauf hingewiesen, dass als Rechtsgrundlage einer Personalaktendatenübermittlung nur die Einwilligung der Betroffenen in Betracht kommt oder eine neue gesetzliche Grundlage geschaffen werden müsse. Über die ersten umfänglichen Beratungen im Zeitraum des IX. Tätigkeitsberichts zum seinerzeitigen Personalservicecenter (PSC) wurde unter Nr. 17.9 berichtet. In der Stellungnahme der Landesregierung hierzu hieß es: „Auch dem Hinweis des LfD, dass bei der Erhebung von Personalaktendaten ohne Einwilligung der Betroffenen die begrenzten Übermittlungsregelungen des § 88 des Landesbeamtengesetzes i. V. m. § 28 DSG LSA zu beachten sind, wird Rechnung getragen. Personalaktendaten werden seitens des PSC ohne Einwilligung der Betroffenen nicht erhoben.“

§ 88 LBG LSA grenzt die Übermittlung von Personalaktendaten stark ein: „Ohne Einwilligung der Beamtin oder des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde, dem Landespersonalausschuss oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das Gleiche gilt für andere Behörden desselben oder eines anderen Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken ha-

ben.“ Die Vorschrift dient u. a. dem Datenzugang von nicht personalaktenführenden Dienststellen, die bei einer konkreten Personalmaßnahme zu beteiligen sind, wenn das Einverständnis des Betroffenen fehlt, wie z. B. bei der Versetzung wider Willen. Hier muss die aufnehmende Stelle sich unter Einsicht in die Personalakten vorbereiten können. Zu denken wäre auch an konkrete Zustimmungsvorbehalte, die einer Personalmaßnahme zunächst entgegen stehen. Die Aufgaben der PVS haben aber allgemeinen, den gesamten benannten Personenkreis betreffenden Charakter. Eine beteiligungspflichtige Personalmaßnahme ist zunächst nicht im Ansatz in Sicht.

Im Zeitraum des X. Tätigkeitsberichts wurden die Beratungen mit der seinerzeit zuständigen Staatskanzlei fortgesetzt. Es wurde erläutert, dass die Tätigkeit einer PVS sinnvoll und die dortige Datenverarbeitung unproblematisch sei. Die Übermittlung von Daten an die PVS bedarf aber einer Rechtsgrundlage. Auf das Verfahren in anderen Ländern (gesetzliche Grundlage oder Einwilligung) wurde schriftlich hingewiesen. Daher sollte zunächst auch weiter auf der Grundlage der Einwilligung gearbeitet werden.

Auf den Hinweis, dass der geplante Erlass Bedenken begegnet, teilte das nun zuständige Ministerium der Finanzen mit, dass man von der Rechtmäßigkeit des Verfahrens ausgehe, aber dennoch an einer Neuregelung arbeite. Der Landesbeauftragte solle darüber informiert werden. Auf eine gebotene Beteiligung bei der Ausarbeitung und die erbetene Ablichtung des verwendeten Vordrucks wartet der Landesbeauftragte seit Monaten.

Zwischenzeitlich ist über eine Landtagsdrucksache (6/2362) bekannt geworden, dass im Rahmen des Entwurfs eines Haushaltsbegleitgesetzes für das Jahr 2014 eine Änderung von § 88 LBG LSA vorgesehen ist, die eine ressortübergreifende Übermittlung von Personalaktendaten an eine Personalvermittlungsstelle gestattet; die Regelung ist unausgereift; der Landesbeauftragte wurde gesetzeswidrig nicht beteiligt.

11.2 Eingliederungsmanagement

In seinem X. Tätigkeitsbericht (Nr. 18.4) hatte der Landesbeauftragte eine Entscheidung des Bundesverwaltungsgerichts dargestellt, deren Verallgemeinerungsfähigkeit fraglich schien. Obergerichtliche Entscheidungen waren danach davon abgewichen.

Nunmehr hat das Bundesverwaltungsgericht (Beschluss vom 4. September 2012, Az.: 6 P 5.11; NZA-RR 2013, 164) ohne Bindung an eine vorinstanzliche Entscheidung und ohne einschränkende Formulierung seine Entscheidung aus dem Jahr 2010 bestätigt. Danach ist die Dienststelle verpflichtet, einem von der Personalvertretung benannten Mitglied in regelmäßigen Abständen mitzuteilen, welche Beschäftigten innerhalb eines Jahres länger als sechs Wochen arbeitsunfähig waren sowie dem Mitglied Einsicht in die Anschreiben an die Betroffenen zu gewähren.

Das Zustimmungserfordernis des § 84 SGB IX beziehe sich nicht auf das Angebot, sondern nur auf die zweite Phase des Eingliederungsmanagements.

Die anlassunabhängige Übermittlung der Namensliste und Einsicht in die Anschreiben sei für die Wahrnehmung der Überwachungsaufgabe erforderlich. Die Mitteilung anonymisierter Unterlagen reiche nicht aus.

Der personalvertretungsrechtliche Informationsanspruch begrenzt insoweit das Grundrecht der Betroffenen auf informationelle Selbstbestimmung. Die Kontrolle der Personalvertretung diene dem Schutz der Betroffenen vor dem Verlust ihrer Arbeitsplätze, die Wiedereingliederung betreffe ein elementares Gemeinschaftsinteresse. Das Gewicht der betroffenen Gesundheitsdaten sei gering, da nur die Tatsache der Voraussetzungen nach § 84 Abs. 2 Satz 1 SGB IX, nicht aber die exakte Dauer der Abwesenheit bekannt werde. Zudem sei die Abwesenheit regelmäßig ohnehin bekannt, sodass meist nur noch die Privatanschrift zur Kenntnis gelangt.

Nach der Erfahrung des Landesbeauftragten gestalten einige Personalvertretungen ihre Kontrolle nach § 84 Abs. 2 Satz 7 SGB IX datenschutzfreundlicher und machen den oben dargestellten Anspruch nicht geltend. Aus datenschutzrechtlicher Sicht bleibt es erfreulicherweise dabei, dass lediglich eine weitere Person zu informieren ist. Die Begrenzung auf eine Person war nach der Begründung des Bundesverwaltungsgerichts für die Abwägung von entscheidender Bedeutung (Rn 38 des Beschlusses).

11.3 Aufbewahrung von Abmahnungen

Bei der Prüfung eines Personalamtes stellte der Landesbeauftragte fest, dass das Personalamt dazu übergegangen war, Abmahnungen dauerhaft in Personalakten zu speichern. Hierzu wurde auf Folgendes hingewiesen:

Der Anspruch auf Entfernung einer unberechtigten Abmahnung ist in der Rechtsprechung des Bundesarbeitsgerichts seit langem anerkannt. Die Aufbewahrung von zunächst berechtigten Abmahnungen gestaltet sich problematischer.

Es ergibt sich schon aus der (ggf. entsprechenden) Anwendung der §§ 89 Abs. 1 Satz 1 Nr. 2 LBG LSA i. V. m. 28 Abs. 1 DSG LSA, dass begründete Abmahnungen i. d. R. nach zwei Jahren aus der Personalakte zu entfernen sind.

Denn Behauptungen, Beschwerden oder Bewertungen, die für den Betroffenen ungünstig sind oder nachteilig werden können, sind nach zwei Jahren auf Antrag zu entfernen. Abmahnungen, die ein Verhalten als vertragswidrig bewerten und die Aufforderung zu pflichtgemäßem Verhalten statuieren, dürften unter diese Regelung fallen. Dafür spricht auch, dass diese Entfernungsregelung nach § 16 Abs. 5 DG LSA ebenfalls für das beamtenrechtliche Pendent zur Abmahnung, die schriftliche Missbilligung, gilt.

Auch nach der Rechtsprechung des Bundesarbeitsgerichts kann grundsätzlich ein Anspruch auf Entfernung zunächst berechtigter Abmahnungen bestehen, wenn sie für die weitere Beurteilung überflüssig geworden sind (durch Zeitablauf „verbraucht“). Ein solcher Fall liegt vor, wenn eine Interessenabwägung im Einzelfall ergibt, dass die weitere Aufbewahrung zu unzumutbaren beruflichen Nachteilen für den Arbeitnehmer führen könnte, obwohl der beurkundete Vorgang für das Arbeitsverhältnis rechtlich bedeutungslos geworden ist. Eine zur Personalakte genommene Abmahnung ist geeignet, den Arbeitnehmer in seinem beruflichen Fortkommen und seinem Persönlichkeitsrecht zu beeinträchtigen.

Da die Rechtsprechung bei derartigen Auseinandersetzungen auch auf den langjährigen Vorrat an Vertrauen abstellt, hat auch der Dienstherr bzw. Arbeitgeber ein Interesse, sich bei Kündigungsverfahren auf Vertrauensverlust infolge früheren Fehlverhaltens berufen zu können. Hier können ggf. auch länger zurück liegende Abmahnungen eine Rolle spielen.

Die Abmahnung hat dem Bundesarbeitsgericht zufolge nicht nur eine Warnfunktion, sondern auch eine Rüge- und Dokumentationsfunktion. Ein Anspruch auf Entfernung setzt nicht nur den zeit- und verhaltensbedingten Verlust der Warnfunktion voraus. Auch sonstige berechtigte Interessen an der Dokumentation der Pflichtverletzung sind zu beachten.

Bei der in diesen Fällen gebotenen Interessenabwägung ist in Sachsen-Anhalt die Wertung des Gesetzgebers in den Vorschriften des § 89 Abs. 1 Satz 1 Nr. 2 LBG LSA i. V. m. § 28 Abs. 1 DSG LSA und § 16 Abs. 5 DG LSA zu berücksichtigen. Die pauschale dauerhafte Aufbewahrung von Abmahnungen erscheint daher unzulässig.

11.4 Verplappert

Ein Blumengeschäft hatte einem Vater auf telefonische Anfrage, warum man das Ausbildungsverhältnis seiner Tochter gekündigt habe, mitgeteilt, dass die Tochter selbst gekündigt hatte. Darüber beklagte sich die Tochter beim Landesbeauftragten.

Bei der Weitergabe von Informationen zur Kündigung an den Vater handelte es sich um eine Datenübermittlung, die einer Rechtsgrundlage bedurfte.

Eine Einwilligung lag nicht vor. Auch auf der Grundlage des BDSG war die Information an den Vater nicht zulässig. Dies wäre nur der Fall gewesen, wenn sie zur ordnungsgemäßen Beendigung des Beschäftigungsverhältnisses erforderlich gewesen wäre. Zwar mag es ein berechtigtes Interesse des Blumengeschäfts gegeben haben, gegenüber einem Anrufer die Behauptung, man hätte gekündigt, richtig zu stellen. Dennoch vermag dies im Verhältnis zum Interesse der Betroffenen die Erforderlichkeit nicht zu begründen. Die Informationen zum Beginn oder zur Beendigung eines Beschäftigungsverhältnisses sind sensible Informationen zu einem wesentlichen Lebensabschnitt, zu dem die Steuerung der Bekanntgabe grundsätzlich nur der Betroffenen zukommt. Auch im familiären Kreis gibt es nicht

selten Gründe, die Information gezielt zu verwenden oder zu verschweigen.

11.5 Überwachung von Notruftelefonaten

Ein Beamter im Einsatzleitzentrum einer Feuerwehr beschwerte sich beim Landesbeauftragten darüber, dass sein Schichtleiter eingehende Notruftelefonate mit anhört, ohne ihn darüber informiert zu haben.

Die um Stellungnahme gebetene Stadt teilte daraufhin mit, dass das Mithören auf einer entsprechenden Dienstanweisung beruhe und dem Mitarbeiter automatisch ein Symbol in Form eines Ohres auf dem Display seines Computers angezeigt werde, wenn der Schichtführer mithört. Darüber hinaus teilte die Stadt mit, dass das Mithören einerseits zur Qualitätssicherung diene und andererseits bei der Anrufannahme gleich verhindert werden solle, dass fehlerhafte Notrufe angenommen würden. So wäre es möglich, fehlerhafte Entscheidungen noch vor der Alarmierung der Einsatzkräfte zu korrigieren.

Der Beschwerdeführer wies darauf hin, dass es sich bei dem eingeblendeten Symbol um eine fünf bis zehn Millimeter kleine Abbildung eines Ohres, das lediglich auf „Ebene 1“ zu sehen sei, handele. Ein Disponent hätte aber mehrere Ebenen zur Verfügung und außerdem auch noch fünf Bildschirme am Arbeitsplatz. Bei der Fülle von gleichzeitig anfallenden Informationen und Tätigkeiten sei es nicht möglich, diesen einen Bildschirm permanent zu überwachen.

Des Weiteren schaltete sich auch der Personalrat ein und stellte dar, dass bisher mit keinem Mitarbeiter des Einsatzleitzentrums eine Auswertung von mitgehörten Notruftelefonaten erfolgt sei.

Auf die angekündigte überarbeitete Dienstanweisung für das Einsatzleitzentrum hat der Landesbeauftragte ca. zwölf Monate gewartet. Nach Vorlage dieser Dienstanweisung wurde seitens des Landesbeauftragten beispielhaft erläutert, dass personenbezogene Daten nicht schon dann weitergegeben werden dürfen, wenn Gefahrenabwehrbehörden die Dringlichkeit geltend gemacht haben. Ein Amtshilfeersuchen allein reicht nicht. Nur aufgrund einer Rechtsgrundlage ist eine personenbezogene Datenübermittlung zulässig. Diese Dienstanweisung beinhaltete auch, dass im Rahmen der Ausbildung und Qualitätssicherung einzelne Gespräche eines Mitarbeiters aufgezeichnet werden dürfen, wenn dies gemeinsam mit dem Mitarbeiter erfolgt. Hier wurde nicht eindeutig klar, ob damit gemeint ist, die Einwilligung des Mitarbeiters einzuholen. Falls eine Einwilligung eingeholt wird, war fraglich, ob diese im Einzelfall oder generell eingeholt wird und ob die Nutzung zur Weiterbildung nur für diesen einzelnen Mitarbeiter oder auch für andere Mitarbeiter erfolgt.

Nachdem fünf Monate später keine Klärung erfolgte, kontrollierte der Landesbeauftragte vor Ort. Inzwischen erfolgte das Mithören bei Notruftelefonaten nur noch, wenn der Schichtleiter vom Schreibtisch des Disponenten einen weiteren Hörer aufnimmt. Dieser verfügt über einen Schalter durch

den man sich zum Hören, aber auch zum Sprechen in das Telefongespräch einschalten kann. Direkt im Anschluss an das Gespräch, jedoch möglichst in der Schicht, soll dieses mit dem betroffenen Mitarbeiter ausgewertet werden. Im Ergebnis war damit festzustellen, dass das Verfahren seit seiner Umstellung keinen grundsätzlichen datenschutzrechtlichen Bedenken mehr begegnet.

11.6 Mithörfunktionen von dienstlichen Telefonanlagen

Durch Pressemitteilungen wurde der Landesbeauftragte auf den Verdacht des Missbrauchs (Mithören, Babyphone-Funktion) dienstlicher Telefonanlagen bei der Polizei eines anderen Landes aufmerksam. Auf Nachfrage hat das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt dazu Folgendes mitgeteilt:

Eine Möglichkeit zum Mithören von Telefongesprächen bzw. Gesprächen in Räumen sei nicht bekannt. Die Funktionen „direktes Ansprechen“ sowie „Babyphone“ seien deaktiviert. Ein Aktivieren sei nicht ohne Weiteres möglich und wäre zudem durch optische und akustische Signale erkennbar. Dennoch sei das Technische Polizeiamt veranlasst, verschiedene weitere Leistungsmerkmale mit dem Hersteller der Telefonanlage kritisch auf Missbrauchspotential zu prüfen.

Aufgrund der vielfältigen Funktionen komplexer Telekommunikationsanlagen hält der Landesbeauftragte es ebenso für geboten, die notwendigen technisch-organisatorischen Maßnahmen in Bezug auf dienstliche Telefonanlagen zu treffen, um unzulässigen Verwendungen zu begegnen. Soweit keine spezialgesetzlichen Aufzeichnungsregelungen bestehen, sollten Funktionen mit Missbrauchspotential grundsätzlich deaktiviert sein.

12 Finanzen, Kataster, Kommunales und Statistik

12.1 Auskunftsrecht für Betroffene im Steuerverfahren – Teil III

Die Beauftragten für den Datenschutz des Bundes und der Länder haben sich auch in diesem Tätigkeitsberichtszeitraum (vgl. IX. Tätigkeitsbericht, Nr. 9.1, und X. Tätigkeitsbericht, Nr. 8.1) weiter für eine klare gesetzliche Regelung des Auskunftsrechts für Betroffene im Steuerverfahren eingesetzt.

Das Bundesministerium der Finanzen legte dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Oktober 2011 einen neuen Diskussionsentwurf zur Änderung der Abgabenordnung vor, in dem ein entsprechender Auskunftsanspruch über gespeicherte Daten geregelt werden sollte.

Die Datenschutzbeauftragten des Bundes und der Länder gaben daraufhin eine gemeinsame Stellungnahme gegenüber dem Bundesministerium der Finanzen ab, in der sie den neuen Entwurf ausdrücklich begrüßten. So wurde positiv bewertet, dass im neuen Entwurf auf die grundsätzliche

Verpflichtung zur Darlegung eines Informationsinteresses an der Auskunftserteilung verzichtet wurde. Zu einzelnen Punkten wurde jedoch weiterer Ergänzungs- und Änderungsbedarf angemeldet. Dies betraf u. a. die Einfügung eines Absatzes in die neue Regelung, nach welchem die für die Kontrolle des Datenschutzes zuständige Stelle nur mit Zustimmung der verantwortlichen Finanzbehörde eine Auskunft an den Betroffenen erteilen darf. Eine solche Regelung wäre jedoch nicht mit der völligen Unabhängigkeit der Datenschutzbeauftragten zu vereinbaren.

Den Datenschutzbeauftragten des Bundes und der Länder liegt derzeit kein überarbeiteter Entwurf zur Regelung des Auskunftsrechts für Betroffene im Steuerverfahren vor. Der Landesbeauftragte wird das Verfahren weiter beobachten, da in dieser Hinsicht, auch aufgrund aktueller Rechtsprechung im Bereich des Informationszugangsrechts (vgl. II. Tätigkeitsbericht zur Informationsfreiheit, Nr. 6.7.3), Handlungsbedarf besteht.

12.2 Evaluierung des „anderen sicheren Verfahrens“ bei ElsterOnline

Bereits im IX. Tätigkeitsbericht (Nr. 9.7) und im X. Tätigkeitsbericht (Nr. 8.3) berichtete der Landesbeauftragte über die Risiken der unsicheren Authentifizierung bei der ElsterOnline-Anmeldung.

Wie im X. Tätigkeitsbericht erläutert, wurde bei der Evaluierung des „anderen sicheren Verfahrens“ nicht auf die ursprünglich geforderten hohen Schutzanforderungen bei einer elektronischen Übermittlung der Daten der Steuererklärung durch eine qualifizierte elektronische Signatur eingegangen. Für die Evaluierung kam es nicht mehr auf die Sicherstellung der Integrität des übermittelten Dokuments an, sondern nur auf die Zuordnung des übersandten Dokuments zu einem Nutzerkonto. Dies wurde zwar von den Datenschutzbeauftragten des Bundes und der Länder kritisiert, diese Kritik fand jedoch im Evaluierungsbericht keine Berücksichtigung, da der gesetzliche Auftrag darauf beschränkt war, nur das „andere sichere Verfahren“ zu beurteilen. Nach Aussage des Bundesministeriums der Finanzen sind bei der Prüfung des „anderen sicheren Verfahrens“ keine Missbrauchsfälle bekannt geworden.

Als Folge des Evaluierungsverfahrens wurde durch das Steuervereinfachungsgesetz 2011 § 87a Abs. 6 der Abgabenordnung dahingehend geändert, dass neben der qualifizierten elektronischen Signatur im Steuerverfahren auch ein anderes sicheres Verfahren zugelassen wird, das den Datenübermittler authentifiziert und die Integrität des elektronisch übermittelten Datensatzes gewährleistet. Insbesondere der neue Personalausweis (nPA) soll zukünftig zur Authentifizierung eingesetzt werden.

Das ElsterOnline-Portal ist eine Website, auf welcher Bürgerinnen und Bürger u. a. ihre Steuererklärungen online ausfüllen und absenden können. Seit Anfang 2013 ist eine Registrierung im ElsterOnline-Portal auch mit Hilfe des sog. nPA möglich. Dieser dient dazu, die Identität des sich registrierenden Nutzers zu überprüfen. Das Verschicken von Briefen mit Zugangsdaten (sog. Aktivierungsbriefe) entfällt somit, sodass diese Web-

site ohne Wartezeit sofort genutzt werden kann. Die Nutzung weiterer elektronischer Dienste, wie die Abfrage der Elektronischen Lohnsteuerabzugsmerkmale oder der Elektronische Einspruch, ist möglich. Das Diensteangebot des Portals könnte zukünftig noch umfangreicher werden.

Die zukünftige Möglichkeit der Registrierung mit dem nPA wird dazu führen, dass – neben den anderen angebotenen Zugangsverfahren mittels Software-Zertifikat oder USB-Token – das dritte Zugangsverfahren mit Signaturkarte und damit die qualifizierte elektronische Signatur verdrängt werden wird. Die qualifizierte elektronische Signatur dient dazu, Dokumente mit einer rechtsverbindlichen elektronischen Unterschrift zu versehen. Kritisch bei der Nutzung einer solchen Unterschrift zur Anmeldung am ElsterOnline-Portal ist die Möglichkeit des Missbrauchs. Der nPA wurde u. a. dafür geschaffen, die eigene Identität im Internet elektronisch nachweisen zu können. Insofern ist die Wahl des nPA als allgemein verfügbare Authentifizierungskomponente richtig. Die eID-Funktion des nPA ist jedoch kein Ersatz für eine elektronische Unterschrift mittels qualifizierter elektronischer Signatur. Er kann nämlich die Integrität der übertragenen Daten nicht garantieren. Der nPA wird jedoch noch nicht zur Anmeldung am ElsterOnline-Portal, sondern nur zur Registrierung genutzt. Zur Anmeldung wird derzeit auf die drei genannten Zugangsverfahren zurückgegriffen.

In der Praxis zeigt sich zudem, dass andere, sichere Verfahren oft deshalb kaum genutzt werden, weil es noch ein einfacher zu handhabendes Verfahren gibt – z. B. das Versenden von Daten ohne jede Authentifizierung. Dazu bieten Programme mit der Elster-Komponente zur Abgabe der Steuererklärung die Möglichkeit der einfachen Übertragung auf den Server der Finanzverwaltung an. Diese Möglichkeit ist teilweise sogar bereits in den Programmen voreingestellt. Es ist nachvollziehbar, dass sich Nutzer einer Software – z. B. für die Steuererklärung – in der Regel keine Zeit nehmen, sich aufwändig zu registrieren, ihren nPA freischalten zu lassen, sich USB-Token zusenden zu lassen oder Software-Zertifikate zu beantragen, wenn entsprechende Programme die Übertragung auch ohne Authentifizierung ermöglichen. Die Zuordnung der übertragenen Daten aus solchen Programmen zum Nutzer erfolgt später anhand eines gedruckten und unterschriebenen Papierdokuments, das die Stamm- und Übertragungsdaten des Nutzers enthält.

Der Landesbeauftragte weist darauf hin, dass ein immer stärkeres Vereinfachen und Aufweichen der Verfahren dazu führen wird, dass auch Angriffe auf diese immer einfacher erfolgen können. Es sollten Mindestsicherheitsstandards etabliert werden. Das „andere sichere Verfahren“ mit nPA und verschlüsselter Kommunikation mit dem Server der Finanzverwaltung sollte vollständig offengelegt und durch unabhängige Dritte evaluiert werden. Das Übersenden von Daten ohne Authentifizierung sollte nicht mehr ermöglicht werden.

12.3 Steuer-ID

Durch sein Urteil vom 18. Januar 2012 (DuD 2012, 275) bestätigte der Bundesfinanzhof, dass die Zuteilung und Speicherung der Steuer-Identifikationsnummer (Steuer-ID) nicht gegen das Recht auf informationelle Selbstbestimmung verstößt.

Der Bundesfinanzhof erkannte in seiner Begründung des Urteils durchaus an, dass durch die Vergabe einer Steuer-ID und deren zentrale Speicherung ein Eingriff in das informationelle Selbstbestimmungsrecht gegeben ist. Schließlich werden die Finanzbehörden durch die mit der Steuer-ID ermöglichte eindeutige Identifizierung des Steuerpflichtigen in die Lage versetzt, mit Hilfe der elektronischen Datenverarbeitung alle Möglichkeiten auszuschöpfen und zulässige Überprüfungen umfassend durchzuführen. Ein solcher Eingriff darf nur auf Grund einer verfassungsmäßigen gesetzlichen Grundlage erfolgen, die mit §§ 139a, 139b AO vorliegt.

Der Bundesfinanzhof stellte in seiner Begründung des Urteils dazu fest, dass mit der Steuer-ID auf effektive Weise sowohl die Festsetzung wie auch die Erhebung von Steuern für Belastungsgleichheit sorgt und somit ein Allgemeingut gewährleistet wird. Des Weiteren ist die Belastung des Einzelnen durch die Vergabe, die Speicherung und die Nutzung der zu der Steuer-ID gespeicherten Daten relativ gering. Es kann durch die Daten, die zu einer natürlichen Person gespeichert werden, kein Persönlichkeitsprofil gebildet werden. Es handelt sich auch nicht um eine unzulässige Vorratsdatenspeicherung, da die Zwecke, zu denen die Steuer-ID erhoben wird, im Gesetz geregelt sind. Der durch die Erhebung der Steuer-ID erfolgte Grundrechtseingriff ist somit abzuwägen gegen die angestrebten Ziele, die mit der Erhebung und Speicherung der Steuer-ID zu erreichen sind. Dabei stellte der Bundesfinanzhof fest, dass eine, den Steuerpflichtigen weniger belastende, aber gleich effektive Alternative nicht zur Verfügung steht.

Gleichwohl bleibt die Gefahr der Entwicklung der Steuer-ID zu einem Personenkennzeichen nicht gebannt (so auch der Bundestag in seinem Beschluss vom 13. Juni 2013, BT-Drs. 17/13936, Nr. 9).

12.4 Auskünfte aus dem Liegenschaftskataster

Aus einem anderen Land war dem Landesbeauftragten über den dort praktizierten inflationären Umgang mit den personenbezogenen Daten aus dem Liegenschaftskataster berichtet worden. Unter Hinweis auf ihr unternehmenszweckbedingtes berechtigtes Interesse hätten dort im Bereich des Immobilienverkehrs tätige Unternehmen bei der Katasterbehörde massenhaft Auskünfte zu Liegenschaften – also Grundstücken – samt den Eigentümerangaben angefordert und wohl auch bekommen. Genutzt wurden die Eigentümerangaben, um Verkaufsobjekte für die Vermittler- und Maklertätigkeit zu gewinnen. Den Eigentümern war dies nicht recht. Sie fühlten sich belästigt und sorgten sich um die wohl von der Katasterverwaltung freizügig herausgegebenen Eigentümerangaben. Adressat der

Beschwerden dieser Betroffenen war der Datenschutzbeauftragte ihres Landes.

So verschärft besteht das Problem in Sachsen-Anhalt offenbar nicht. Es gab beim Landesbeauftragten einzelne Beschwerden über Kontaktaufnahmen durch Makler, die auf dem Wege der Kaltakquise Verkaufsobjekte für solvente Kunden gewinnen wollten. Da das im Umkehrschluss nicht bedeuten musste, dass das aus dem anderen Land bekanntgewordene Problem nicht doch auch in Sachsen-Anhalt bestehen könnte, fragte der Landesbeauftragte beim Landesamt für Vermessung und Geoinformation (LVermGeo) die tatsächlich geübte Verfahrensweise an.

Rechtsgrundlage für die Benutzung des Liegenschaftskatasters in Sachsen-Anhalt ist § 13 VermGeoG LSA. Nach § 13 Abs. 1 Satz 2 VermGeoG LSA erhalten Auskunft und Auszüge aus Liegenschaftsbuch und Liegenschaftskarte auch andere Personen, soweit sie ein berechtigtes Interesse daran darlegen und öffentliche Belange dem nicht entgegenstehen. Damit fällt sofort die Parallelität zu § 12 Abs. 1 Satz 1 GBO ins Auge, nach dem Einsicht in das Grundbuch jedem gestattet ist, der ein berechtigtes Interesse darlegt.

Daraus wird zunächst deutlich, dass der Gesetzgeber Liegenschaftskataster und Grundbuch eine nur begrenzte Publizität zuspricht, im Gegensatz beispielsweise zum Handelsregister oder zum Schuldnerverzeichnis, die jeweils uneingeschränkt öffentlich sind. „Ein berechtigtes Interesse ist ein nach vernünftiger Abwägung durch die Sachlage gerechtfertigtes Interesse, das rechtlicher, wirtschaftlicher oder ideeller Natur sein kann.“, so wortgleich Horber/Demharter, GBO, Kommentar, 20. Auflage 1993, § 12 Anmerkung 7 ff., und Eyermann-Fröhler, VwGO, 9. Auflage, § 43 Rn 11. Dieses berechtigte Interesse sprechen Kummer/Möllering, Kommentar zum Vermessungs- und Katasterrecht Sachsen-Anhalt, 2. Auflage, § 13 VermKatG LSA, Anmerkung 3.4.5 solchen natürlichen und juristischen Personen zu, die beruflich mit Bau- und Grundstücksangelegenheiten befasst sind, darunter auch Makler aufgrund eines bestehenden Maklervertrages im Rahmen einer Einzelauskunft. Sie sehen jedoch für Makler kein allgemeines Auskunftsrecht bei einer undifferenzierten Massenauskunft, z. B. über die Namen der Grundstückseigentümer ganzer Straßenzüge, wenn keine konkreten Beziehungen zu den Eigentümern bestehen. Kein berechtigtes Interesse sei auch gegeben bei bloßer Bauplatzsuche ohne vorherige Vertragsverhandlungen. Diese Auffassung wird vom Landesbeauftragten und LVermGeo geteilt, und eine Auskunftserteilung aus dem Liegenschaftskataster offenbar auch restriktiv gehandhabt – damit datenschutzgerecht.

In diesem Zusammenhang datenschutzrechtlich durchaus interessant ist auch ein anderer Aspekt: Dadurch, dass das Liegenschaftskataster nach § 13 VermGeoG LSA ein – wenn auch beschränkt – öffentliches Register darstellt, bei dem mit den gesetzlichen Einschränkungen ein Benutzungsanspruch durch Inhaber anerkannt berechtigter Interessen besteht, bietet sich im Gegenzug für die Grundstückseigentümer kein Raum, diesen Be-

nutzungsanspruch, z. B. von Unternehmen der Immobilienwirtschaft, durch Widerspruch zu beschränken.

12.5 Kommunalverwaltung

12.5.1 Schiedsstellen

Aus Anlass der Änderung der Verwaltungsvorschriften zum Schiedsstellen- und Schlichtungsgesetz, bei welcher der Landesbeauftragte Empfehlungen zur datenschutzrechtlichen Gestaltung insbesondere technischer Aspekte geben konnte, wurde eine Schiedsstelle geprüft. Im Rahmen dieser Kontrolle stand die tatsächliche Praxis der Schiedsstelle beim Umgang mit den bekanntgewordenen personenbezogenen Daten im Mittelpunkt.

Besonders positiv war zu bewerten, dass regelmäßige Schulungen durch das zuständige Amtsgericht durchgeführt wurden und somit die Schiedspersonen in ihrer Arbeit nicht auf sich allein gestellt waren.

Die Formulare, die für die Arbeit der Schiedspersonen genutzt wurden, werden vom Bund Deutscher Schiedsmänner und Schiedsfrauen zur Verfügung gestellt. Diese sind speziell auf die Rechtslage in Sachsen-Anhalt abgestimmt. Felder für Angaben in den Formularen, die von den Schiedspersonen als nicht notwendig angesehen wurden, konnten frei gelassen oder für andere sinnvolle Hinweise genutzt werden. Zum Beispiel wurde im Feld „Personalausweisnummer“ nur der Hinweis „ausgewiesen durch PA“ vermerkt. So konnte auf die Speicherung personenbezogener Daten, die für die Arbeit nicht erforderlich sind, verzichtet werden.

Ein Problem, das jedoch nicht allein durch den Landesbeauftragten für den Datenschutz geklärt werden konnte, war die Unterbringung der Akten nach Abschluss des eigentlichen Verfahrens. Nach der Justizaufbewahrungsordnung besteht in der Regel eine Aufbewahrungspflicht von 30 Jahren für Akten über Verfahren nach dem Schiedsstellen- und Schlichtungsgesetz. Es wurde festgestellt, dass Akten teilweise nicht in den Diensträumen der Kommune gelagert wurden, sondern in den Privaträumen der Schiedspersonen. Aus diesem Grunde müsste eine gesonderte Regelung für die Aufbewahrung der abgeschlossenen Verfahren mit der jeweiligen Kommune bzw. mit dem jeweiligen Amtsgericht getroffen werden.

12.5.2 Abwasserzweckverbände

In der letzten Zeit häuften sich die Anfragen von Bürgerinnen und Bürgern, ob erneute Datenerhebungen der Abwasserzweckverbände zulässig seien. Dabei wurde ausgeführt, dass die Daten den Abwasserzweckverbänden bereits bekannt seien. In den meisten Fällen ging es aber darum, dass die Abwasserzweckverbände Erhebungsbögen zur Erfassung der Niederschlagswassermengen versandten, die dann von den Grundstücksbesitzern ausgefüllt und an externe Firmen zur Auswertung gesandt werden sollten.

Für die Zulässigkeit der Datenerhebung und -verarbeitung kommt es darauf an, ob die jeweilige Satzung des Abwasserzweckverbandes diese regelt.

Zum einen muss in der Satzung eine Regelung für die Erhebung von Niederschlagswassergebühren enthalten sein. Der Abwasserzweckverband darf personenbezogene Daten nur erheben, wenn sie zur Aufgabenerfüllung erforderlich sind. Ist also dem Abwasserzweckverband durch die Verbandsversammlung die Aufgabe der Abwasserbeseitigung übertragen worden, jedoch noch keine Satzungsänderung erfolgt, dafür auch Gebühren zu erheben, dürfen nur die Daten erhoben werden, die für die Berechnung der Niederschlagsmengen und die Kapazität der Leitungen erforderlich sind. Hierzu dürften zum Teil auch Schätzungen genügen. Sollen jedoch auch Niederschlagswassergebühren erhoben werden, dann muss in der Satzung die Berechnungsgrundlage festgelegt werden, um eine gleichmäßige Gebührenfestsetzung zu ermöglichen. Wenn diese gegeben ist, dürfen aus datenschutzrechtlicher Sicht auch die genauen Angaben der Grundstückseigentümer erhoben werden.

Zum anderen muss durch die Satzung die Möglichkeit eröffnet sein, dass Aufgaben an Dritte übertragen werden dürfen. Bei den durch den Landesbeauftragten erfolgten Prüfungen war dies der Fall. Dann muss der Abwasserzweckverband mit der jeweiligen Fremdfirma einen Vertrag zur Datenverarbeitung im Auftrag schließen. Dabei bleibt der Abwasserzweckverband der Verantwortliche für die Datenverarbeitung. Zur Vertragsgestaltung kann auf den Mustervertrag zu Auftragsverhältnissen nach § 8 DSG LSA zurückgegriffen werden.

12.5.3 Einschaltung von Inkassobüros

Die Vollstreckung kommunaler Forderungen unter Inanspruchnahme von Inkassobüros wurde im VIII. Tätigkeitsbericht (Nr. 11.2) bereits erörtert. Die zugrundeliegenden Fragen werden in der fachlichen Diskussion auch derzeit nicht einheitlich beantwortet. Maßgeblich dürfte eine differenzierte Prüfung im Einzelfall sein.

Für privatrechtliche Forderungen ist davon auszugehen, dass eine Abtretung nach § 398 BGB möglich ist. Die der Abtretung zugrundeliegende schuldrechtliche Verpflichtung beinhaltet auch die Übergabe der für die Geltendmachung erforderlichen Informationen. Aus Gründen der Datensparsamkeit sollte jedoch an Stelle des Inkassobüros vorrangig der eigene Außendienst eingesetzt werden.

Im Hinblick auf öffentlich-rechtliche Forderungen ist zwischen der Aufgabenübertragung und der Datenverarbeitung im Auftrag zu unterscheiden.

Eine Aufgabenübertragung wird grundsätzlich als unzulässig angesehen. Die Regelungen der Gemeindeordnungen, welche die Übertragung von Kassengeschäften an Dritte vorsehen, stellen keine Rechtsgrundlage für die Übertragung von hoheitlichen Aufgaben dar. Die Beitreibung von Geldforderungen im Verwaltungszwangsverfahren ist Teil der Eingriffsverwal-

tung und bedarf einer spezifischen Grundlage. Die Übertragung auf Private ist spezialgesetzlich nicht vorgesehen.

Der Beteiligung von Dritten bei der Einziehung öffentlich-rechtlicher Forderungen im Wege der Datenverarbeitung im Auftrag stehen durchaus einige Bedenken entgegen. Die Beitreibung ist grundsätzlich Aufgabe der öffentlichen Stelle. Das Verwaltungsverfahrensrecht fordert, Geheimnisse der Betroffenen, insbesondere sensible Schuldnerdaten, soweit wie möglich geheim zu halten. Zu berücksichtigen ist auch, dass eine ordnungsgemäße und sichere Erledigung von Forderungsmanagementaufgaben durch Inkassobüros in der Praxis nicht immer ganz unproblematisch ist. Die Büros sind zumeist auch auf dem Gebiet des Auskunfteiwesens tätig, eventuellen Vorteilen (aktuellere Adressdaten) stehen Umsetzungsnachteile entgegen, da das Instrumentarium des Verwaltungsvollstreckungsrechts nicht zur Verfügung steht und legal handelnde Inkassobüros keine Sanktionsmöglichkeiten haben.

Dennoch erscheint die Übertragung bestimmter Aufgaben auf Inkassounternehmen im Wege der Datenverarbeitung im Auftrag insgesamt zumindest als vertretbar. Die Beauftragung von Verwaltungshelfern ist nicht von vorn herein ausgeschlossen. Es muss sich aber um eine reine Verarbeitung von Daten im Sinne der Datenverarbeitung im Auftrag handeln. Die Aufträge müssen klar und eindeutig formuliert sein und die tatsächliche Umsetzung auch dem Wortlaut entsprechen. Hilfstätigkeiten wie die Adressermittlung oder das Mahnwesen können so übertragen werden, Bonitätsprüfungen und eine gewisse Korrespondenz könnten ggf. auch zulässig sein.

Die vollständige Übertragung von Aufgaben im Sinne einer Überwachung des Zahlungsverkehrs, der Bearbeitung von Widersprüchen und Stundungen, der Durchsetzung der Forderungen sowie der Entscheidung über das Vorgehen im Einzelfall und der konkreten Ausgestaltung der dabei zu treffenden Maßnahmen ist unzulässig. Die in konkreten Situationen zu treffenden Entscheidungen sind durch die Kommune vorzugeben.

So ist auch darauf zu achten, dass eine unüberwindbare Trennung der Datenbestände und Organisationseinheiten beim Auftragnehmer gewährleistet ist. Die Einbeziehung von Daten kommunaler Schuldner in den Auskunfteibereich soll vermieden werden. Dem Inkassobüro dürfen nur Informationen in beschränktem Umfang für die Wahrnehmung des Auftrags übergeben werden. Informationen über das Schuldverhältnis und die Art der Forderung sollten dem Auftragnehmer nur mitgeteilt werden, soweit dies zur Erfüllung des Auftrags erforderlich ist.

Zudem ist zu bedenken, dass ggf. spezielle Vorschriften für eine Auftragsdatenverarbeitung einschlägig sein können (vgl. § 80 SGB X). Dies gilt auch für Vorgänge nach dem Unterhaltsvorschussrecht. Auch sind besondere Amts- oder Berufsgeheimnisse zu berücksichtigen (ärztliche Schweigepflicht, Personalaktengeheimnis).

12.6 Statistik – Auswertung Zensus 2011

Der registergestützte Zensus 2011 – die Bevölkerungs-, Gebäude- und Wohnungszählung mit dem Stichtag 9. Mai 2011 – kann mit Fug und Recht als das europäische Statistikprojekt des Jahrzehnts angesehen werden. Über die Erhebungsvorbereitung und vor allem die dabei zu Tage getretenen datenschutz- und statistikrechtlichen Probleme und, soweit dies gelang, ihre Lösung hatte der Landesbeauftragte in seinem X. Tätigkeitsbericht (Nr. 23.1) ausführlich berichtet.

Der aktuelle Berichtszeitraum war im Zusammenhang mit dem Zensus 2011 zunächst von Kontrollen von Erhebungsstellen – in Sachsen-Anhalt existierten 37 solche Stellen – geprägt. Die dabei aufgetretenen Unzulänglichkeiten ließen sich in allen Fällen rasch beheben. So war z. B. in einem Fall versäumt worden, die Erhebungsbeauftragten gem. § 10 Abs. 2 ZensG 2011 i. V. m. § 3 Abs. 3 ZensAG LSA auf das Statistikgeheimnis zu verpflichten. Die in § 4 Abs. 1 bis 4 ZensAG LSA vorgeschriebenen Maßnahmen zur Trennung der örtlichen Erhebungsstellen von den anderen Verwaltungsbereichen mussten gem. § 4 Abs. 5 ZensAG LSA in einer Dienstanweisung durch den Bürgermeister der Gemeinde schriftlich festgelegt werden. In einem Fall war das unterblieben, d. h. man arbeitete dort „freihändig“. Es zeigte sich, dass die Dienstanweisung längst fertig, durch den Bürgermeister jedoch noch nicht in Kraft gesetzt worden war. Auch IT-seitige Unzulänglichkeiten wurden festgestellt. Der Virenscanner eines Erhebungsstellen-PC war durch den Nutzer deaktivierbar, als Speicherort für Office-Dateien war häufig der Ordner „Eigene Dateien“ im lokalen Laufwerk – also fernab jedes Backup-Verfahrens – voreingestellt.

Zeitaufwendiger war die datenschutzrechtliche Bearbeitung der Beschwerden der vom Zensus 2011 Betroffenen. Hierbei gab es zum Teil einfache Sachverhalte, wie z. B. auf dem Postweg verloren gegangene Erhebungsbögen, Einwürfe in falsche Hausbriefkästen oder Verknüpfungen Betroffener mit längst nicht mehr in deren Eigentum stehenden Wohnungen oder Häusern infolge veralteter Datenbestände.

Ein Bürger hat sich gegen die Auskunftspflicht bei der Frage nach seiner rechtlichen Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft gewandt (§ 7 Abs. 4 Nr. 19 ZensG 2011). Der Landesbeauftragte wies Ihn auf Art. 136 Abs. 3 WRV, der nach Art. 140 GG Bestandteil des Grundgesetzes ist, hin. Danach haben Behörden das Recht, nach der Zugehörigkeit zu einer Religionsgesellschaft zu fragen, sofern eine gesetzlich angeordnete statistische Erhebung dies erfordert.

Problematischer war der Fall eines Ortsbürgermeisters, der zum Erhebungsbeauftragten in seiner eigenen Gemeinde bestellt worden war, obwohl er nach § 6 Abs. 3 ZensAG LSA durch seine Berufs- und sonstigen in seiner Person liegenden Umstände – er ist schließlich nicht nur Vertrauensperson, sondern auch Exekutivorgan – an der Übernahme der Tätigkeit als Erhebungsbeauftragter gehindert gewesen wäre. Nach § 11 Abs. 3 ZensG 2011 hätte er auch nicht in der Nähe seiner eigenen Woh-

nung eingesetzt werden dürfen. In dieser nur sehr kurz währenden Tätigkeit hatte er auch noch den Fehler begangen, einen Erhebungsbogen zur GWZ nach § 6 ZensG 2011 an einen Betroffenen durch Niederlegung bei der Wirtin einer Gaststätte zuzustellen.

Doch nach dem Zensus ist vor dem Zensus. Voraussichtlich wird auch im Jahre 2021 eine entsprechende statistische Erhebung durchgeführt werden. Im Hinblick auf diese Erhebung hatte der Arbeitskreis Statistik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe gebildet, die unter Mitwirkung des Landesbeauftragten eine Zusammenstellung von Aspekten für die weitere Diskussion über eine Novellierung des BStatG und die Durchführung statistischer Erhebungen – insbesondere des nächsten Zensus – erörterte. Der Landesbeauftragte hat u. a. folgende Vorschläge zur Verbesserung der Regelungen und Verfahren eingebracht:

Vollerhebung bei der Gebäude- und Wohnungszählung (GWZ)

Der Bestandteil GWZ des Zensus 2011 war als Vollerhebung durchgeführt worden. Der Landesbeauftragte vertritt den Standpunkt, dass – wie bei der Haushaltsstichprobe – auch bei der GWZ eine Stichprobe in Höhe von 10 % ausreichend sein dürfte. Der Verordnung (EG) Nr. 763/2008 über Volks- und Wohnungszählungen, die den Zensus 2011 anordnete, ist eine Pflicht zur Vollerhebung jedenfalls nicht zu entnehmen.

Erhebung von Personen, die freiwillig im Melderegister angemeldet sind

Nach § 3 Abs. 1 ZensG 2011 haben die Meldebehörden den Statistischen Ämtern der Länder für jede gemeldete Person die im Gesetz bestimmten Daten zu übermitteln. Unter § 3 Abs. 1 Nr. 25 ZensG 2011 findet sich die Angabe „Information über freiwillige Anmeldung im Melderegister“. Dabei handelt es sich um Personen, die entsprechend internationaler Abkommen im Gastland nicht zu zählen sind, z. B. Mitglieder ausländischer Streitkräfte und deren Angehörige, Diplomaten, Mitglieder berufskonsularischer Vertretungen usw. Diese können sich freiwillig registrieren lassen. Die Daten dieser Personen wurden beim Zensus 2011 von der amtlichen Statistik ohne jedes Erfordernis erhoben, was zukünftig unterbleiben sollte.

Übermittlungssperre und deren Grund (§ 3 Abs. 1 Nr. 26 ZensG 2011)

Um die Haushaltsstichprobe ohne übermittlungsgesperrte Personen generieren zu können, ist möglicherweise in § 3 Abs. 1 Nr. 26 ZensG 2011 angeordnet worden, den Statistischen Ämtern der Länder von den Meldebehörden zu den Personen, für die eine melderechtliche Auskunfts- und Übermittlungssperre (§ 35 Abs. 2 MG LSA) eingerichtet ist, die Tatsache des Bestehens dieser Übermittlungssperre und zu allem Überfluss den Grund der Übermittlungssperre zu übermitteln.

Die Erfahrungen zeigten, dass die statistikfehlerfreie Haushaltsstichprobe ohne Anschriften von übermittlungsgesperrten Personen nicht zu erzeugen war. Die Angabe (§ 3 Abs. 1 Nr. 26 ZensG 2011) wurde letztlich ignoriert. Ihr Vorhandensein führte lediglich zu Unsicherheiten bei allen Betei-

ligten, nicht zuletzt bei den Betroffenen (vgl. X. Tätigkeitsbericht, Nr. 23.1.4). Die Tatsache des Bestehens einer Übermittlungssperre und insbesondere auch ihr Grund sollten zukünftig in der amtlichen Statistik nicht mehr verwendet werden.

Erhebungen in Sonderbereichen

In der Begründung des Gesetzentwurfes zum Zensusvorbereitungsgesetz (BT-Drs. 16/5525) war noch angekündigt worden, die Erhebung in sensiblen Sonderbereichen anonym durchzuführen, was aber im Laufe der Beratungen vom Bundesinnenministerium unter Hinweis auf die gebotene Qualitätssicherung verworfen wurde. Das Ergebnis war schließlich in § 8 ZensG 2011 zu finden, wo u. a. Vor- und Familiennamen, die Geburtsdaten, Geschlecht und Familienstand als Erhebungs- bzw. Hilfsmerkmale erfasst sind.

Zu unterscheiden sind Sonderbereiche mit hohen Fluktuationsraten und unterdurchschnittlich ausgeprägter Meldemotivation. Vorstellbar wäre das in Studentenwohnheimen oder Flüchtlingsunterkünften. Dort mag eine personenbezogene Erhebung im Sinne von § 8 ZensG 2011 gerechtfertigt sein.

Im Gegensatz dazu ist die personenbezogene Erhebung in Justizvollzugsanstalten, Erziehungsheimen – gerade bei geschlossener Unterbringung – und Klöstern als nicht gerechtfertigt zu sehen (sensible Sonderbereiche). Der Landesbeauftragte hält es für abwegig zu behaupten, die Leiter dieser Einrichtungen könnten nicht angeben, wie viele männliche und weibliche Personen mit welchen Familienständen und welchen Alters bei ihnen untergebracht sind, ohne personenbezogene Daten zu übermitteln. Dass diese Personen auch andernorts gemeldet sind, ist dagegen eher unwahrscheinlich. Hier bietet eine Differenzierung einen Ansatzpunkt für eine datenschutzrechtliche Verbesserung des Zensusanordnungsgesetzes (2021).

Verkürzter Melderegisterauszug nach § 11 Abs. 11 ZensG 2011 für Erhebungsbeauftragte

Die Erhebungsbeauftragten erhalten danach zur Unterstützung ihrer Tätigkeit bei den Erhebungen einen verkürzten Melderegisterauszug für die betreffenden Anschriften. Dieser Auszug soll u. a. den Tag der Geburt jeder dort gemeldeten Person enthalten. Dabei meint Tag der Geburt wohl nicht den Tag der Geburt im Sinne von § 8 Abs. 2 Nr. 2b ZensG 2011, sondern eher das komplette Geburtsdatum, wie es nach § 3 Abs. 1 Nr. 5 ZensG 2011 zu verstehen ist.

In den vom Landesbeauftragten kontrollierten Erhebungsstellen war stets abweichend von der gesetzlichen Vorschrift lediglich das Jahr der Geburt auf den Melderegisterauszügen enthalten. Das hatte stets genügt, um die Person exakt zu bestimmen und war datenschutzgerecht im Sinne der Datensparsamkeit. Diese Abwandlung sollte zukünftig Gesetzeskraft erlangen.

Übermittlung von Einzelangaben an kommunale Statistikstellen

Nach § 22 Abs. 2 ZensG 2011 dürfen die Statistischen Ämter den kommunalen Statistikstellen für ausschließlich statistische Zwecke auf Blockseitenebene – eine Blockseite ist ein Straßenabschnitt zwischen zwei Einmündungen – aggregierte Einzelangaben und auch Einzelangaben zu den Hilfsmerkmalen „Straße“ und „Hausnummer“ übermitteln. Ob die adressscharfe Übermittlung von Einzelangaben datenschutzrechtlich zulässig ist, bedarf jedenfalls noch einmal der Diskussion, ebenso wie die Frage, ob die blockseitenaggregierten Daten in den kommunalen Statistikstellen ohne Zeitbegrenzung gespeichert werden dürfen.

Allerdings war es nicht möglich, in Bezug auf alle Details Einvernehmen zwischen den Datenschutzbeauftragten des Bundes und der Länder herzustellen, sodass eine Veröffentlichung durch die Datenschutzkonferenz nicht möglich war. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat deshalb ein eigenes Eckpunktepapier im zeitlichen Zusammenhang mit der Veröffentlichung der ersten Zensus-Ergebnisse Ende Mai 2013 herausgeben.

13 Wirtschaft und Verkehr

13.1 Düsseldorfer Kreis

Der Düsseldorfer Kreis ist ein bundesweites Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Vertreter dieser Behörden waren im Herbst 1977 in Düsseldorf erstmals zusammengekommen, um sich auf eine möglichst einheitliche Anwendung des damals neu erlassenen Bundesdatenschutzgesetzes (BDSG) zu verständigen.

Da die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich in Deutschland ursprünglich nicht einheitlich geregelt war, gehörten je nach Landesrecht die Landesbeauftragten für den Datenschutz als auch die Innenministerien zu den Mitgliedern des Düsseldorfer Kreises. Nachdem der Europäische Gerichtshof im Jahr 2010 entschieden hat, dass die Datenschutzaufsicht im nicht-öffentlichen Bereich schon wegen der potentiellen Gefahr einer politischen Einflussnahme nicht – wie es in Deutschland bisher teilweise üblich war – in den Zuständigkeitsbereich eines Ministeriums fallen kann, sondern völlig unabhängig sein muss (EuGH, Urteil vom 9. März 2010, Az.: C-518/07, NJW 2010, 1265), haben die Länder die Datenschutzaufsicht neu geregelt. Mit Ausnahme von Bayern haben alle Länder den Landesbeauftragten für den Datenschutz die Kontrolle des BDSG übertragen. In Bayern nimmt diese Aufgabe das Bayerische Landesamt für Datenschutzaufsicht wahr.

Infolge der gesetzlichen Neuregelung der Zuständigkeiten der Aufsichtsbehörden wurde auch der Düsseldorfer Kreis reformiert. Aufgrund der Mitgliedschaft der Innenministerien hatte sich der Düsseldorfer Kreis bisher selbständig und unabhängig von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder über die Auslegung des BDSG ver-

ständigt. Nachdem die Datenschutzbeauftragten des Bundes und der Länder für die Kontrolle der Einhaltung des Datenschutzes im öffentlichen wie auch im nicht-öffentlichen Bereich zuständig sind, wurde der Düsseldorfer Kreis in die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Datenschutzkonferenz) integriert.

Der Düsseldorfer Kreis ist ein besonderer Arbeitskreis der Datenschutzkonferenz. Er soll die Konferenz von Einzelfragen zur Auslegungspraxis entlasten, zur Koordinierung der Aufsichtspraxis in Bund und Ländern beitragen und in diesem Rahmen weiterhin Verhandlungen mit der Wirtschaft führen. Ziel des Düsseldorfer Kreises als in der föderalen Aufsichtsstruktur etabliertes „Markenzeichen“ bleibt die bundesweit einheitliche Auslegung des geltenden Rechts im nicht-öffentlichen Bereich in wesentlichen Fragen sowie die Verständigung zwischen den Aufsichtsbehörden über ein aufsichtsbehördliches Vorgehen, um zu einem verlässlichen, bundesweit möglichst einheitlich angewandten Datenschutzniveau im nicht-öffentlichen Bereich zu gelangen. Soweit es um die Auslegung des geltenden Rechts geht, ist der Kreis dabei befugt, eigenständige Beschlüsse zu treffen, die veröffentlicht werden, wenn sie ohne Gegenstimmen zustande kommen.

In Angelegenheiten mit datenschutzpolitischem Hintergrund bzw. datenschutzpolitischen Forderungen kann er Beschlüsse fassen, die in Form einer Entschließungsempfehlung der Datenschutzkonferenz vorgelegt werden. Diese besitzt insofern die Letztentscheidungskompetenz.

Eine Besonderheit des Düsseldorfer Kreises besteht darin, dass an seinen Sitzungen bei Bedarf Vertreter des Bundesministeriums des Innern als auch der Innenministerien der Länder als Gäste teilnehmen können. Hierdurch wird der Informationsaustausch zwischen den Datenschutzbehörden und den Innenressorts des Bundes und der Länder auch nach der erfolgten Umstrukturierung aufrecht erhalten.

13.1.1 Themen und Arbeitsgruppen

Als wichtige Arbeitsgruppen (AG) des Düsseldorfer Kreises sind beispielsweise die AG Versicherungswirtschaft, die AG Auskunfteien, die AG Kreditwirtschaft, die AG Sanktionen, die Ad-hoc-AG elektronisches Lastschriftverfahren, die AG Internationaler Datenverkehr oder die Ad-hoc-AG Werbung und Adresshandel zu nennen. Die Arbeitsgruppen verständigen sich u. a. über die Auslegung des geltenden Datenschutzrechts, verhandeln mit der Wirtschaft und bereiten Beschlüsse des Düsseldorfer Kreises vor.

Zu den wesentlichen Beiträgen des Düsseldorfer Kreises zählen im Berichtszeitraum insbesondere die Beschlüsse

- zur Videoüberwachung in und an Taxis (vgl. Nr. 4.17.5),
- zum Datenschutz in sozialen Netzwerken (vgl. Nr. 4.19),

- zur Near Field Communication (NFC) bei Geldkarten (vgl. Nr. 13.1.4),

- zum anonymen und pseudonymen elektronischen Bezahlen von Internet-Angeboten (vgl. Nr. 13.1.5) und

- zur Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft (vgl. Nr. 13.3).

Für die Werbung und den Adresshandel hat der Düsseldorfer Kreis eine Orientierungshilfe herausgegeben.

Eine immer größere Bedeutung erlangen ferner sog. Verhaltensregeln (Code of Conducts – CoC), die Berufsverbände oder andere Vereinigungen der zuständigen Aufsichtsbehörde zur Prüfung der Vereinbarkeit mit dem geltenden Datenschutzrecht vorlegen können. Diese Verhaltensregeln sollen die Einhaltung des bestehenden Datenschutzrechts in der jeweils spezifischen Branche fördern und Rechtssicherheit im Hinblick auf branchentypische Datenflüsse schaffen.

Der Düsseldorfer Kreis hat in diesem Zusammenhang eine Orientierungshilfe für Unternehmensverbände, die sich entsprechende Verhaltensregeln geben wollen, entwickelt (**Anlage 33**).

Die Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft stellen ein wichtiges Beispiel für die Praxis dar (vgl. Nr. 13.3). Auch die Geodaten verarbeitende Industrie plant, für ihre Branche entsprechende Verhaltensregeln zu entwickeln; die Beratungen durch den Düsseldorfer Kreis dauern noch an (vgl. Nr. 13.1.3).

13.1.2 Informationspflicht bei Datenpannen

Nach **§ 42a BDSG** haben nicht-öffentliche Stellen die Pflicht zur Anzeige an den Landesbeauftragten als Aufsichtsbehörde, wenn sie feststellen, dass bestimmte bei ihr gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Umfasst sind personenbezogene Daten besonderer Art (§ 3 Abs. 9 BDSG), Daten, die einem Berufsgeheimnis unterliegen, Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den diesbezüglichen Verdacht beziehen oder Daten zu Bank- und Kreditkartenkonten. Weitere Voraussetzung der Anzeigepflicht ist, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Daher muss das einzelne Unternehmen eine Gefahrenprognose vornehmen und die Frage erheblicher materieller oder sozialer Schäden prüfen und die Eintrittswahrscheinlichkeit ermitteln. Bei Vorliegen der Voraussetzungen sind weitere Handlungen geboten, wie etwa Maßnahmen zur Minderung möglicher nachteiliger Folgen und die Benachrichtigung der Betroffenen. Detaillierte Informationen zu den wichtigsten Fragen finden sich unter anderem auf der Homepage des Berliner Beauftragten für den Datenschutz und Informationsfreiheit (www.datenschutz-berlin.de) unter dem Thema „Informationspflicht bei Datenlecks“ sowie des Landesbeauft-

ragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (www.ldi.nrw.de). Der Düsseldorfer Kreis nahm das vom Berliner Beauftragten erstellte Merkblatt zu Mitteilungen nach § 42a BDSG zustimmend zur Kenntnis. Es ist auf der Seite des Landesbeauftragten verlinkt.

Auch zu dieser Thematik gingen Anfragen beim Landesbeauftragten ein. Ein Beispiel war der Transfer von Patientendaten zu einem Unternehmen, das die von ihm hergestellten Medizingeräte fernwartet. Hierzu hatte sich letztlich durch Prüfungen in anderen Ländern herausgestellt, dass keine schwerwiegenden Beeinträchtigungen zu befürchten waren. Dennoch war der Vorgang Anlass, auf die Notwendigkeit der sorgsamen Ausgestaltung von Auftragsdatenverarbeitungen hinzuwirken.

Das Bundesministerium des Innern plante – parallel zu Vorstellungen der EU-Kommission zu einer Netz- und Informationssicherheitsstrategie – die Schaffung eines IT-Sicherheitsgesetzes mit Meldepflichten für Betreiber kritischer Infrastrukturen und TK-Unternehmen (vgl. Friedrich, MMR 2013, 273, und Beucher/Utzerath, MMR 2013, 362). Der Entwurf erreichte nicht mehr die parlamentarische Reife; die Wirtschaft empfahl den Weg freiwilliger Mindeststandards für mehr Cyber-Sicherheit.

Teilweise überholt wurde die Entwicklung durch die Verordnung 611/2013 der EU-Kommission vom 24. Juni 2013 über Maßnahmen für die Benachrichtigung der Datenschutzbehörde bei Datenschutzverletzungen durch Telekommunikationsanbieter (in Umsetzung der E-Privacy-Richtline 2002/58/EG).

13.1.3 Geoinformation

In der wirtschaftlichen Nutzung staatlicher Geoinformationen, also der Nutzung dieser Daten durch die Wirtschaft, liegt ein hohes Wertschöpfungspotential. Der Landesbeauftragte berichtete in seinem X. Tätigkeitsbericht unter Nr. 11.1 und ferner unter Nr. 3.1.3 bereits darüber.

Von entscheidender Bedeutung ist in diesem Zusammenhang die Frage, welche Geodaten von öffentlichen Stellen in welcher Form an die interessierten Wirtschaftsunternehmen herausgegeben werden können, ohne mit datenschutzrechtlichen Vorschriften in Kollision zu geraten und wie die Wirtschaftsunternehmen mit den erhaltenen und durch Verarbeitung oder Weiterbearbeitung gewonnenen Daten umgehen. Der dabei durch die öffentlichen Stellen zu führende Abwägungsprozess ist nicht immer einfach. Er könnte Unterstützung finden, wenn sich die Wirtschaftsunternehmen durch Festlegen von Verhaltensregeln nach § 38a BDSG eine Selbstverpflichtung in Bezug auf den Umgang mit diesen Daten auferlegen würden (**Anlage 33**). Diese Idee der Selbstverpflichtung würde nicht nur die Entscheidungsprozesse der öffentlichen Stellen vereinfachen, sondern auch die Eigenverantwortung der Wirtschaft stärken.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat im Auftrag der GIW-Kommission im Rahmen der Machbarkeitsstudie „Be-

reitstellung von Geodaten unter Berücksichtigung datenschutzrechtlicher Aspekte anhand des Datenclusters Denkmalschutz der öffentlichen Verwaltung für die Wirtschaft“ ein Gutachten dazu erstellt.

Diese sich für alle Beteiligten bietende Chance der Eigenverantwortung der Wirtschaft hatte bereits im Jahre 2010 die GIW-Kommission erkannt und die TaskForce „GeoBusiness Datenschutz“ ins Leben gerufen, in der der Landesbeauftragte seit ihrer Einrichtung im September 2010 mitarbeitet. Seitdem war die TaskForce der Frage nachgegangen, welche Rolle Verhaltensregeln nach § 38a BDSG spielen könnten.

Im Verlaufe einer Vielzahl von Beratungen der TaskForce, oft gemeinsam mit der Unterarbeitsgruppe Geodaten des Arbeitskreises Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, war schließlich im Berichtszeitraum ein Memorandum Geobusiness und Datenschutz erarbeitet worden. Dieses Memorandum mit dem zunächst sperrigen Titel „Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen betreffend die Nutzung von Geodaten und Geodatendiensten der öffentlichen Hand durch Wirtschaftsunternehmen“ wurde später „Geobusiness CoC“ genannt. Es darf im Übrigen nicht verwechselt werden mit dem Datenschutz-Kodex für Geodatendienste (vgl. X. Tätigkeitsbericht, Nrn. 1.2 und 3.1.3), der für Panoramadienste bestimmt ist.

Im Zuge der Beratungen des Memorandums wurde dieses neben dem CoC um einen weiteren Teil ergänzt, und zwar um die „Hinweise und Empfehlungen für die Bereitstellung von Geodatendiensten und die Übermittlung von Geodaten durch Behörden und sonstige öffentliche Stellen des Bundes und der Länder“. Dieser Teil sollte die Form einer Orientierungshilfe erhalten, CoC und Orientierungshilfe sich gegenseitig ergänzen.

Allerdings traten bei den Beratungen des Memorandums durch die Unterarbeitsgruppe (UAG) Geodaten und die TaskForce GeoBusiness Datenschutz auch schwer zu überwindende Differenzen, nicht nur zwischen den Datenschutzbeauftragten und den Vertretern der Wirtschaft, sondern selbst zwischen den Datenschutzbeauftragten zutage. Der Grund lag u. a. darin, dass die Landesbeauftragten die inkompatible Rechtslage in ihren jeweiligen Zuständigkeitsbereichen im Blick hatten. Dies wird an folgendem Beispiel deutlich:

Nach der Rechtslage in Sachsen-Anhalt ist der Zugang zu Geodaten zu beschränken, soweit durch sie personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. In anderen Ländern wird der Informationszugang für die Wirtschaft dagegen erst gesperrt, wenn eine erhebliche Beeinträchtigung der Betroffenen vorliegt. Hier ist der Schutz also schwächer als in Sachsen-Anhalt (z. B. in Baden-Württemberg, Bremen oder Nordrhein-Westfalen).

Da beabsichtigt war, die Orientierungshilfe durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Kraft setzen und den CoC vom Düsseldorfer Kreis bestätigen zu lassen, wurden die einzel-

nen Teile des Entwurfs des Memorandums diesen Gremien vorgelegt mit dem Ergebnis, dass wegen nicht gegebener Beschlussreife eine Zurücküberweisung an die UAG Geodaten und die TaskForce GeoBusiness Datenschutz zur Überarbeitung erfolgte.

13.1.4 Mobiles kontaktloses Bezahlen

Die Near Field Communication (NFC)-Technologie entwickelt sich zum anbieterübergreifend genutzten Übertragungsstandard zur drahtlosen Bezahlung. Sie erlaubt einen kontaktlosen Datenaustausch im Nahbereich. Dieser beträgt normalerweise nur etwa „3 bis 5“ Zentimeter, aber auch bei einem Anbieter laut Selbstauskunft „bis zu ca. einem halben Meter“. Insbesondere der Handel und die Automatenwirtschaft haben ein großes Interesse an der Nutzung dieses kontaktlosen Bezahlverfahrens. Teilweise bieten sie es bereits an Kassen aller Art an. Banken und Sparkassen bieten Karten mit NFC-Funktion unter verschiedenen Namen an. Bei den Sparkassen werden diese für Geldbeträge bis 20 Euro genutzt. Über eine Handy-App bzw. im Handel mit einem passenden Kartenlesegerät lassen sich die letzten 15 Bezahltransaktionen und die letzten 3 Aufladungen anzeigen. Grundsätzliche Zielstellung ist, dass dies anonym und sicher funktionieren soll. In Zukunft werden weitere Funktionen beispielsweise für die Handy-Apps erwartet. Diese sollen dann auch die kontaktlose Geldbörse aufladen können oder mobile Zahlungsvorgänge via Handy ermöglichen. Auch die Kreditkartenanbieter verfügen über Anwendungen und Verfahren zur kontaktlosen Bezahlung. Mit dem Thema NFC beschäftigen sich sowohl die Arbeitsgruppe Kreditwirtschaft des Düsseldorfer Kreises als auch der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder seit längerem.

Mobiles Bezahlen ist mittlerweile auch mit Hilfe von mobilen Kartenlesegeräten möglich. Hier ist der Kartenleser mit dem Smartphone des Händlers verbunden. Die Abrechnung erfolgt über eine Drittfirma. Problematisch ist der Umstand, dass Daten von z. B. Kreditkarten durch Schadsoftware auf dem Smartphone abgefangen werden können. Hier müssen insbesondere die Smartphone-Hersteller dafür sorgen, dass Anwendungen und deren Daten besser vor unberechtigten Zugriffen von Fremdanwendungen abgeschirmt werden.

Das Touch&Travel-System der Deutschen Bahn AG steht allen Kunden seit November 2011 zur Verfügung. Seit Dezember 2012 ist die generelle Nutzung NFC-fähiger Handys neben beispielsweise manuellen oder QR-Code-basierten Eingaben möglich. Leider geht der Komfortgewinn zu Lasten des Datenschutzes, denn es wird ein detailliertes Kundenprofil aufgebaut. Mehr noch, der Reisende muss sein Handy eingeschaltet lassen, damit ein Bewegungsprofil (Mobilfunkzellen bzw. GPS-basiert) erstellt werden kann. Denkbar wäre es alternativ auch, dass ein Kunde ohne Nachverfolgung durch die Deutsche Bahn AG reist und sich nur an Start-, Halte- und Endpunkten am System anmeldet, das Bewegungsprofil aber beim Kunden hinterlegt und nicht an die Bahn transferiert wird. Ein Missbrauch könnte auch durch vorherige Festlegung eines Reiseziels im Handy ausgeschlossen werden. Hier ist die Papierfahrkarte eindeutig im Vor-

teil. In Japan werden derartige Kundenprofile bereits an andere Unternehmen verkauft. Ein solches Szenario sollte in Deutschland verhindert werden.

Alle drahtlosen (kontaktlosen) Kommunikationsverfahren erlauben mehr oder weniger einfach das unberechtigte Mitlesen des Roh-Datenstroms. Es ist deshalb wichtig, mit technisch-organisatorischen Maßnahmen wie zeitgemäßer Verschlüsselung und Mehrfaktor-Authentisierung zu verhindern, dass personenbezogene Daten offenbart werden. Ansonsten besteht eventuell die Möglichkeit, dass Kartennummern, Geldbeträge oder vergangene Transaktionen unberechtigt auslesbar sind, weil auf angemessene Schutzmaßnahmen verzichtet wurde. Nutzer sollten die NFC-Funktionen der Karten aktivieren und deaktivieren und die Betrags-Limits passend setzen können (hierauf weist auch der Düsseldorfer Kreis in seinem Beschluss vom 18./19. September 2012 hin, vgl. **Anlage 31**). Als Alternative hierzu bieten zurzeit kontaktbehaftete Verfahren mehr Sicherheit.

Eine datenschutzgerechte Umsetzung von kontaktlosen Bezahlangeboten ist nur möglich, wenn diese bereits bei der Entwicklung entsprechend gestaltet wurden. Ein positiver, auch durch die Datenschutzbeauftragten des Bundes und der Länder begleiteter Prozess, ist die Anwendung des Privacy Impact Assessment (PIA) durch Unternehmen selbst. Hier sind beispielhaft die PIAs der Geldkarte der Deutschen Kreditwirtschaft (girogo), der kontaktlosen Zahlungsverfahren von VISA (PayWave) und von MasterCard (PayPass) zu nennen. Durch eine systematische Analyse der Auswirkungen einer Anwendung oder eines Verfahrens auf die Privatsphäre und den Datenschutz, mittels eines PIA (Datenschutzfolgeabschätzung), besteht bei richtiger Umsetzung die Möglichkeit für Unternehmen, datenschutzgerechte Technologien zu entwickeln. Ziel des PIA ist es auch, die Unternehmen anzuhalten, „Privacy-by-Design“ sicherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder werden in ihren Arbeitsgremien die Entwicklung weiter konstruktiv beratend, aber auch kritisch begleiten.

13.1.5 Anonymes und pseudonymes Bezahlen von Internetangeboten

Zunehmend werden im Internet Inhalte gegen Bezahlung angeboten. Die Tendenz geht dahin, Inhalte und Daten auch zu niedrigen Preisen zu verkaufen, sodass hier detaillierte Kunden- und Nutzungsprofile entstehen. Nutzer müssen sich jedoch im Internet unbeobachtet bewegen und Inhalte zur Kenntnis nehmen können.

Gemäß § 13 Abs. 6 Telemediengesetz hat der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Des Weiteren ist der Nutzer über diese Möglichkeit zu informieren. Bei vielen Telemedien-Anbietern werden die Daten aber gemeinsam erfasst und genutzt. Konsum und Zahlung verschmelzen immer mehr. Daher weist der Landesbeauftragte darauf hin, dass eine Bezahlung von Inhalten nicht da-

zu führen darf, dass die Anonymität des Nutzers aus diesem Grund aufgegeben wird. Der Abruf kostenpflichtiger Inhalte sollte ohne die Erfassung personenbeziehbarer Daten über jeden einzelnen Abruf erfolgen können.

Im Berichtszeitraum hat der Bundesgesetzgeber mit dem Gesetz zur Optimierung der Geldwäscheprävention vom 22. Dezember 2011 (BGBl. I S. 2959) weitere Regelungen zur Prävention gegen Geldwäsche getroffen. Sowohl im Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 13. August 2008 (BGBl. I 2008 S. 1690) als auch in der Richtlinie 2005/60/EG vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung („dritte Geldwäscherichtlinie“, ABl. L 309 S. 15) sind Pflichten zur Identifizierung des Vertragspartners beispielsweise im Falle der „Begründung einer Geschäftsbeziehung“ enthalten. Dies wird oft als zu allgemein kritisiert. Eine generelle Identifizierungspflicht würde dazu führen, dass anonymes Bezahlen selbst von Bagatellbeträgen im Internet oder die Benutzung von Prepaidkarten unmöglich würde. Da elektronisches Geld als „digitale Währung“ für den Handel im Internet und mobil per Smartphones prädestiniert ist, wird es in Zukunft eine zunehmend bedeutendere Rolle spielen. Die Datenschutzbeauftragten des Bundes und der Länder forderten mit ihrer Entschließung „Anonymes elektronisches Bezahlen muss möglich bleiben“ vom 28. September 2011 (**Anlage 8**), dass zumindest ein Grenzwert für Bagatellbeträge, bis zu welchem anonymes Bezahlen möglich ist, eingeführt werden sollte. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) fassten am 22. November 2011 in einem Beschluss ihre Forderungen nach der Erhaltung anonymer und pseudonymer Bezahlmöglichkeiten zusammen (**Anlage 28**).

Mit dem vorstehend genannten Gesetz zur Optimierung der Geldwäscheprävention wurde das Kreditwesengesetz (KWG) nach Hinweisen auch seitens der Datenschützer angepasst. Unter anderem wurde in § 25i Abs. 2 KWG ein Maximalwert von 100 Euro pro Kalendermonat aufgenommen (vgl. Nr. 5.2). Bis zu diesem Betrag ist der Umtausch in E-Geld oder ein Erwerb von E-Geld-Trägern bedingt, aber anonym möglich. Die o. g. EU-Richtlinie („dritte Geldwäscherichtlinie“) lässt in Art. 11 Abs. 5 d) den Mitgliedstaaten noch Spielraum für eigene Ausnahmeregelungen und erlaubt in Bezug auf E-Geld eine Bagatellgrenze von 150 Euro. In einem von der Europäischen Kommission eingebrachten Vorschlag für eine Richtline des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung („vierte Geldwäscherichtlinie“) vom 5. Februar 2013 (COM(2013) 45 final) ist dieser Schwellenwert jedoch entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Entwicklung – gerade auch auf europäischer Ebene – weiterhin kritisch beobachten. Die mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder erreichte 100-Euro-Grenze, bis zu der bedingt anonymes Bezahlen möglich ist, wäre bei Wirksamwerden dieses Richtlinienvorschlages der Europäischen Kommission in Gefahr. Letztendlich

würde das zu einer vollständigen Identifizierungspflicht führen und anonyme Prepaid-Angebote und Zahlungen in der EU nicht mehr ermöglichen. Mit diesem Entwurf ist die Europäische Kommission weit über das berechtigte Ziel der Geldwäscheprävention hinaus geschossen.

Eine virtuelle Währung wie z. B. Bitcoin, ein Open-Source-Softwareprojekt für die gleichnamige digitale Währung auf Peer-to-Peer Basis, das hierfür eine Public-Key-Infrastruktur nutzt, ist unabhängig von Zentralbanken und Staaten und dem üblichen Finanzsystem und u. a. damit besonders für den internationalen Geldtransfer geeignet. Über sog. Bitcoin-Adressen kann Geld anonym von einer Wallet-Datei (der eigentlichen Geldbörse des Nutzers) bzw. einem speziellen Service über das Netzwerk an andere Adressen überwiesen werden. Der Besitz von solcher digitaler Währung ist i. d. R. verbunden mit dem Besitz von kryptographischen Schlüsseln. Es ist keineswegs so, dass E-Geld einer erhöhten Gefahr der Geldwäsche oder Nutzung in der Illegalität unterliegen würde und daher die Nutzung von E-Geld mehr eingeschränkt werden müsste. Vielmehr können Ermittlungsbehörden durchaus Geldtransfers eines ihnen bekannten Nutzers auswerten. Das ist mit Bargeld schwieriger.

Es ist wohl nicht oder nur sehr schwer möglich, Handlungen mit E-Geld zu beschränken oder zu unterbinden. Eine gesetzlich vorgeschriebene Identifizierungspflicht bei der umfangreicheren Nutzung von E-Geld – gleichbedeutend mit einem Verbot anonymen E-Gelds – ist jedoch auch nicht notwendig. Das Bundesfinanzministerium hat Bitcoins als digitale Währung in wesentlichen Punkten rechtlich und steuerlich gebilligt und als „Rechnungseinheiten“ anerkannt, so die Antworten des Bundesfinanzministeriums vom 20. Juni 2013 und vom 7. August 2013 auf Anfragen eines Bundestagsabgeordneten.

Ein anonymes Einkaufen und Bezahlen im Internet sollte auch in Zukunft und auch mit E-Geld möglich bleiben.

13.2 Industrie, Handel, Gewerbe

13.2.1 Datenschutzgerechtes Smart-Metering

In seinem X. Tätigkeitsbericht (Nr. 13.1) hatte sich der Landesbeauftragte ausführlich mit dem Thema Smart Meter bzw. Smart Grids befasst und die stärkere Beachtung des Datenschutzes eingefordert, so wie es auch in der damaligen Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. November 2010 zum Ausdruck kam.

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 auch 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 Daten-

umgang 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 muss gem. § 21g Abs. 6 in einer Rechtsverordnung gem. § 21i EnWG geregelt sein, welche die in § 21g EnWG festgelegten Grundsätze zum Datenschutz weiter konkretisieren und detailliert ausgestalten soll. Festzustellen ist allerdings, dass die Bundesregierung von dieser Verordnungsermächtigung, die der Zustimmung des Bundesrates bedarf, bisher keinen Gebrauch gemacht hat.

Am 9. März 2012 hat die Europäische Kommission Empfehlungen zur Vorbereitung für die Einführung intelligenter Messsysteme herausgegeben (Com(2012) 1342 final). Um den Prozess der Erarbeitung und Ausgestaltung der Verordnung gemäß § 21i EnWG zu unterstützen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine „Orientierungshilfe datenschutzgerechtes Smart Metering“ erarbeitet und in einer Umlaufentschließung vom 27. Juni 2012 (**Anlage 14**) bekanntgegeben.

Die Orientierungshilfe gibt Empfehlungen sowohl zur Ausgestaltung der Verordnung als auch zur datenschutzgerechten Konzeption der technischen Systeme für das Smart Metering. Zudem bietet sie Hilfestellungen für die Arbeit der Datenschutzaufsichtsbehörden in den Ländern. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung von Anwendungsfällen (sog. Use Cases) für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Endverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit der Beschreibung der Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Komponenten im Umfeld des Smart Metering erfüllen müssen, sowie der Anforderungen zur Prüfung dieser Eigenschaften in einer Technischen Richtlinie (BSI TR-03109, Version 1.0 vom 18. März 2013) hierfür ebenfalls bereits Vorarbeit geleistet. Gleiches gilt für die vom BSI erstellten Schutzprofile (sog. Protection Profiles) für das Smart Meter Gateway (BSI-CC-PP-0073, Version 1.2 vom 18. März 2013) und für das Security Modul PP (BSI-CC-PP-0077, Version 1.0 vom 18. März 2013).

Es bleibt abzuwarten und zu hoffen, dass die Bundesregierung die Konkretisierung der spezifischen Datenschutzbelange bald in Angriff nimmt, diese Rechtsverordnung erarbeitet und dem Bundesrat zur Abstimmung vorlegt.

13.2.2 Personalausweiskopie

Immer wieder erreichen den Landesbeauftragten die Beschwerden von Bürgern, die auch von der Wirtschaft dazu gedrängt werden, eine Kopie ihres Personalausweises vorzulegen.

Das Kopieren des Personalausweises ist regelmäßig nicht erforderlich, zumal die private Stelle damit auch Daten erhält (wie Zugangs- und Seriennummer, Augenfarbe, Größe), die sie keinesfalls benötigt. Die Vorlage des Personalausweises und ein Vermerk, dass der Ausweis vorgelegen hat, genügen fast immer.

Etwas anderes gilt ausnahmsweise dann, wenn gesetzliche Vorschriften das Kopieren ausdrücklich erlauben oder sogar verlangen (z. B. § 8 Abs. 1 Geldwäschegesetz) oder die persönliche Vorsprache nicht möglich, aber die genaue Identitätsfeststellung notwendig ist (z. B. bei der SCHUFA-Selbstauskunft).

Grundsätzlich ist es nicht mehr möglich, den Personalausweis als „Pfand“ einzubehalten (§ 1 Abs. 1 Satz 3 PAuswG).

13.2.3 Biometrisches Passfoto im Kammerausweis

Eine Kammer verlangte von ihrem Mitglied für die Erstellung eines Kammerausweises ein digitales biometrisches Passfoto. Auf der Grundlage der Europäischen Berufsanerkennungsrichtlinie 2005/36/EG würden europäische Berufsausweise ausgegeben. Der Ausweis sollte bundes- und europaweit einheitlich wie der neue Personalausweis aussehen.

Mit dem sog. biometrischen Passfoto war wohl ein Foto gemeint, das den Anforderungen des § 5 Passverordnung (PassV) i. V. m. ihrer Anlage 8 entspricht. Sinn und Zweck der dort geregelten Abkehr vom Passfoto im Halbprofil auf ein Frontalfoto mit den dort angegebenen Qualitätsanforderungen ist die (biometrische) Auslesbarkeit mit elektronischen Verfahren.

Diese Auslesbarkeit mit elektronischen Verfahren begründet neben einem gewissen Qualitätsgewinn für die Identifizierung jedoch auch erhebliche Risiken im Hinblick auf missbräuchliche Verwendung, beispielsweise durch unberechtigte Kopien. Die Möglichkeit zum Anlegen biometrischer Datensätze betrifft in erheblichem Maße das Persönlichkeitsrecht der Bürgerinnen und Bürger.

Eine spezifische Rechtsgrundlage für die Anforderung schien fraglich. In der Erwägung Nr. 32 der Berufsanerkennungsrichtlinie 2005/36/EG war lediglich vorgegeben, dass die Berufsausweise inhaltliche Informationen, insbesondere zu Qualifikation und beruflichem Werdegang enthalten. Dies soll unter voller Einhaltung der Datenschutzvorschriften erfolgen. Hier war

daher § 1 Abs. 2 Satz 1 DSG LSA (Datensparsamkeit und Datenvermeidung) zu berücksichtigen. Anforderungen an ein Lichtbild oder gar dessen Qualität enthielt die Regelung nicht. Auch das Ingenieurgesetz Sachsen-Anhalt sieht in § 14 Abs. 2 lediglich vor, dass bestimmte Personen einen Ausweis erhalten können. Ein Hinweis darauf, dass ein Passfoto auf dem Niveau nach § 5 PassV zu verwenden sei, fehlte.

Gegen die Verwendung eines Lichtbildes der zuvor genannten Qualität sprach auch, dass in Fällen, in denen dies ausdrücklich gewollt ist, eine spezifische gesetzliche Regelung besteht. So verweist z. B. § 25a Abs. 2 der Fahrerlaubnisverordnung ausdrücklich darauf, dass das Lichtbild der Passverordnung entsprechen muss.

Die Kammer hat auf entsprechende Anfrage mitgeteilt, lediglich auf die Aktualität und die sachgerechte Erkennbarkeit, nicht aber zwingend auf die Standards biometrischer Klassifizierung Wert zu legen.

13.2.4 Recht auf Auskunft über eigene Kundendaten

Manchen Gewerbetreibenden, Unternehmen oder Webseitenbetreibern in Sachsen-Anhalt scheint es nicht geläufig zu sein, dass Betroffene (Kunden) ein unabdingbares und unentgeltliches Recht auf Auskunft über die zu ihrer Person gespeicherten Daten und zu deren Herkunft haben (§ 34 Abs. 1 BDSG). Nur so ist es zu erklären, dass den Landesbeauftragten immer wieder Beschwerden von Bürgern erreichen.

Der Auskunftsanspruch schließt auch Informationen zum Zweck der Speicherung und zu den Empfängern der Daten ein.

Der Landesbeauftragte weist ausdrücklich darauf hin, dass die Nichtbeantwortung oder unvollständige Beantwortung des Auskunftsersuchens von Betroffenen seit September 2009 einen Bußgeldtatbestand erfüllt (§ 43 Abs. 1 Nr. 8a BDSG).

13.2.5 Löschung von Kundendaten

Einigen Bürgern ist unverständlich, dass ihre Kundendaten nicht sofort gelöscht werden (können), wenn sie die Geschäftsbeziehung beenden.

Nach § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Soweit aber gesetzliche, satzungsmäßig oder vertragliche Aufbewahrungsfristen entgegenstehen, tritt an die Stelle einer Löschung eine Sperrung (§ 35 Abs. 3 Nr. 1 BDSG).

Aufbewahrungspflichten ergeben sich für Kaufleute schon aus dem Handelsgesetzbuch, wonach die einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung nachvollziehbar abzubilden sind, und für Steuerpflichtige auch aus der Abgabenordnung.

Sperren ist nach dem Bundesdatenschutzgesetz „das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder

Nutzung einzuschränken“ und für die Bürger das Mittel der Wahl, um ihre personenbezogenen Daten zu schützen.

13.2.6 Bonitätsanfragen bei Auskunfteien

Das neue Handy, eine Bestellung auf Rechnung beim Versandhandel oder ein Kleinkredit – immer besteht ein großes Interesse an der Bonität des betroffenen Kunden.

Dieses wirtschaftliche Interesse wird von unserer Rechtsordnung anerkannt. Deshalb ist die Tätigkeit von Auskunfteien auch grundsätzlich datenschutzrechtlich zulässig. Vertragspartner (Verkäufer bzw. Kreditgeber) dürfen bei nicht beglichenen Forderungen unter den Voraussetzungen des § 28a BDSG den Auskunfteien personenbezogene Daten des Kunden übermitteln. Sie sind aber für die Zulässigkeit der Datenübermittlung verantwortlich.

Der Landesbeauftragte rät allen Bürgern, es gar nicht erst so weit kommen zu lassen: Reagieren Sie unverzüglich auf Mahnbriefe eines Gläubigers und widersprechen Sie ggf. schriftlich der Forderung, sofern sie unberechtigt ist. Ist die Speicherung bei der Auskunftei bereits erfolgt, bitten Sie die Auskunftei schriftlich, sich mit dem Unternehmen, das die Daten übermittelt hat, in Verbindung zu setzen, um den Sachverhalt zu klären und die Daten wieder zu löschen, falls die Voraussetzungen für die Speicherung nicht vorgelegen haben.

13.2.7 Mit OWiSch gegen Schwarzarbeit

Über OWiSch, die Datenbank zur Erfassung von Ordnungswidrigkeiten im Bereich der Schwarzarbeitsbekämpfung, und vor allem über die Probleme, die das zuständige Ministerium für Wissenschaft und Wirtschaft bei deren Einführung in Sachsen-Anhalt verfolgten, hatte der Landesbeauftragte in seinem X. Tätigkeitsbericht (Nr. 13.2) bereits berichtet. Bei der datenschutzrechtlichen Begleitung des Verfahrens war es ihm z. B. wichtig, zu verhindern, dass in OWiSch gespeicherte Personen, gegen die wegen eines bisher unbewiesenen Verdachtes der Schwarzarbeit Ermittlungen geführt werden, gewissermaßen mit einem Stigma behaftet wären und unter Umständen bei der zukünftigen Vergabe öffentlicher Aufträge benachteiligt würden. Dem sei, wie aus dem Ministerium für Wissenschaft und Wirtschaft zu vernehmen war, nicht so. Die Speicherung sei, natürlich als Verdachtsfall, unbedingt erforderlich, denn andernfalls drohe Strafklageverbrauch, wenn zusammenhängende Straftaten nicht als solche erkannt werden.

Ungeklärt ist dagegen weiterhin die 2 Jahre fortwährende Speicherung von Fällen rechtskräftigen Freispruchs des Betroffenen, wenn der Freispruch nicht deshalb erfolgte, weil dieser die Tat nicht begangen hatte. Nach § 49c Abs. 5 OWiG i. V. m. § 489 Abs. 4 Nr. 3 StPO beträgt die Löschfrist maximal 2 Jahre. Weshalb das Ministerium für Wissenschaft und Wirtschaft diese Frist ausschöpfen will, ohne dass ein Speichererfor-

dernis überhaupt besteht, wird der Landesbeauftragte noch zu klären haben.

Da die anderen wesentlichen Bedenken des Landesbeauftragten gegen OWiSch inzwischen ausgeräumt sind, stand dessen Inbetriebnahme nichts mehr im Wege. Der Landesbeauftragte behält sich eine Kontrolle vor, ob das Verfahren datenschutzrechtlich beanstandungsfrei betrieben wird. Mit Kabinettbeschluss vom 13. Dezember 2011 wurde das Ministerium für Wissenschaft und Wirtschaft beauftragt, nach Ablauf von 2 Jahren dem Kabinett über den Nutzen von OWiSch zu berichten. Diesen Bericht erwartet auch der Landesbeauftragte mit großem Interesse.

13.2.8 Betreuung von Kammermitgliedern gegen ihren Willen

Ein Gewerbetreibender, der sein neues Unternehmen pflichtgemäß bei der Kommune angemeldet hatte, bekam wenige Wochen später von seiner Industrie- und Handelskammer (IHK) ein mehrseitiges Begrüßungsschreiben. Die Übermittlung der Daten des Betroffenen aus seiner Gewerbeanzeige von der Kommune an die IHK ist von § 14 Abs. 8 Nr. 1 Satz 1 GewO (damals §14 Abs. 9 Satz 1 Nr. 1 GewO) gedeckt, für die Aufgabenerfüllung der IHK erforderlich und soll hier nicht problematisiert werden.

Der Grund, weshalb sich der Gewerbetreibende an den Landesbeauftragten gewandt hatte, war ein anderer. In den Begrüßungsunterlagen, die die Kammer dem Gewerbetreibenden zugesandt hatte, war auch ein Mitgliederdaten-Fragebogen enthalten. Dieser stellte u. a. Fragen nach der Bankverbindung für Gutschriften, dem Finanzamt und der Betriebssteuernummer und nach Geschäftsbeziehungen ins Ausland. Der Fragebogen diene dazu, so ein Erläuterungsblatt, das IHK-Mitglied in die Auskunfts- und Recherchedatenbank aufnehmen zu können, kostenfrei wohl gemerkt. Nur so könne der Unternehmer schneller als seine Mitbewerber sein.

Falls der Unternehmer jedoch Widerspruch gegen die Weitergabe seiner Daten einlegen wollte, möge er der Kammer das vorgedruckte Formular „Widerspruch zur Weitergabe von Daten“ unterschrieben zurück senden. Dieses Formular enthielt in großer Schrift die Gewerbegrunddaten (Name, Firma inklusive Adresse und Wirtschaftszweig) und in nur 2 mm kleinen Buchstaben folgenden Text: „Hiermit widerspreche ich der Weitergabe der Daten über angebotene Waren und Dienstleistungen, der Daten über die Betriebsgrößenklasse und weiterer Daten aus der Gewerbeanmeldung und/oder dem Handelsregister, die nicht Name, Firma, Anschrift oder Wirtschaftszweig sind, durch die Industrie- und Handelskammer an Dritte.“

Der Unternehmer glaubte nun, durch Nichtausfüllen des Mitgliederfragebogens auch nicht in die Auskunfts- und Recherchedatenbank aufgenommen zu werden, womit sich ein Widerspruch gegen die Weitergabe seiner Daten an Dritte dann wohl erübrige. Damit war der Unternehmer, so musste der Landesbeauftragte ihm auf seine Frage mitteilen, ob das alles datenschutzrechtlich in Ordnung sei, von seiner Kammer schlicht in die Irre geführt worden.

Es gibt nämlich zwischen der in jedem Fall erfolgenden Aufnahme eines Kammermitgliedes in die Auskunfts- und Recherchedatenbank, die eigentlich als Mitgliederverzeichnis der Kammer dient, dem Ausfüllen des Mitgliederfragebogens und dem Widerspruch gegen die Weitergabe – rechtlich eigentlich die Datenübermittlung – bestimmter Daten an Dritte keinerlei Zusammenhang.

Die IHK ist nach § 9 Abs. 4 Satz 1 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) berechtigt, Name, Firma, Anschrift und Wirtschaftszweig von Kammerzugehörigen, also die Gewerbegrunddaten, zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an Dritte zu übermitteln. Widerspruchsmöglichkeit gegen die Übermittlung dieser Daten hat der Gesetzgeber nicht vorgesehen. Die von der Kammer eingeräumte Widerspruchsmöglichkeit richtet sich gegen die Übermittlung der dort genannten besonderen Daten an Dritte. Damit wird die Widerspruchsmöglichkeit aus § 9 Abs. 4 Satz 3 IHK-G realisiert. Durch das Ausfüllen des Mitgliederfragebogens wäre der den Unternehmer betreffende Datensatz also lediglich um die aus dem Fragebogen angegebenen Datenfelder angereichert worden.

Der Landesbeauftragte hat die Kammer gebeten, durch deutliche Formulierungen in den Begrüßungsunterlagen Klarheit für neue Mitglieder zu schaffen.

Die Kammer hatte sich letztendlich sogar dazu entschlossen, „… die Behandlung von Mitgliederdaten über das gesetzliche Maß hinaus …“ zu optimieren. Sie hatte nämlich „zur Vermeidung von Beschwerden“ festgelegt, Mitgliederdaten an nicht-öffentliche Stellen nur noch dann zu übermitteln, wenn das Mitglied hierin ausdrücklich einwilligte. Die übermittelten Daten sind, so teilte die Kammer mit, auf die Gewerbegrunddaten beschränkt, die übrigen in § 9 Abs. 1 IHK-G genannten Daten werden nicht mehr übermittelt. Das ist eine durchaus datenschutzgerechte Lösung. Schließlich ist schwer vorstellbar, wie z. B. das Geburtsdatum eines Unternehmers dem Wirtschaftsverkehr dienen könnte.

13.2.9 Wirksame Übermittlungssperre bei Kammermitgliederdaten der IHK

Für die Erfüllung einer Vielzahl von Aufgaben bedienen die Kammern sich ihrer Gemeinschaftseinrichtungen. Solche Einrichtungen, zu denen auch die IHK Gesellschaft für Informationsverarbeitung mbH (IHK-GfI) gehört und die nach § 9 Abs. 2 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) öffentliche Stellen im Sinne des § 2 Abs. 2 Bundesdatenschutzgesetz sind, dürfen, im Rahmen der Erfüllung der Kammeraufgaben nach § 9 Abs. 3 IHK-G, auch die personenbezogenen Daten der Kammermitglieder verwenden. Das geschieht im Wege der Auftragsdatenverarbeitung nach § 8 DSG LSA. Die IHK-GfI selbst ist also nicht Dritte im Sinne von § 2 Abs. 9 DSG LSA. Eine dieser Kammeraufgaben ist bezeichnenderweise die Mitgliedergrunddaten auf Ersuchen an andere Kammern zu übermitteln. Diese Aufgabe führt die IHK-GfI im Auftrag der Kammer aus.

Der Landesbeauftragte hatte nun untersucht, wie gewährleistet wird, dass auch die IHK-GfI den Wunsch mancher Kammermitglieder nach Nichtübermittlung der Mitgliederdaten an Dritte beachtet. Das sich den Landesbeauftragten festgestellte Ergebnis war datenschutzgerecht. Die Daten, deren Übermittlung an Dritte ein Kammermitglied widersprochen hat, werden im Datenbestand der IHK-GfI mit einem „datenschutzrechtlichen Sperrvermerk“, auch Datenschutzkennzeichen genannt, versehen. Die bei der IHK-GfI verwendete Verwaltungssoftware, im Besonderen das Selektionssystem, verhindert, dass die so gekennzeichneten Datensätze aus dem Gesamtdatenbestand des Servers abgerufen oder gar weitergegeben werden können. Dieses Verfahren hatte bereits im Jahre 2005 durch das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein ein Datenschutzgütesiegel zuerkannt bekommen. Allerdings ist das bis zum Jahre 2007 befristete Gütesiegel danach nicht erneut beantragt worden.

Der Landesbeauftragte begrüßt ausdrücklich, dass hier Datensparsamkeit im Sinne von § 1 Abs. 2 DSG LSA und die Wahrung der Betroffeneninteressen gleichermaßen Beachtung finden.

13.3 Neuregelungen in der Versicherungswirtschaft

Die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen ist weder im Versicherungsvertragsgesetz noch im Bundesdatenschutzgesetz ausreichend geregelt. Also kann sie nur auf der Grundlage einer informierten Einwilligung des Versicherungsnehmers sowie einer Schweigepflichtentbindungserklärung erfolgen. Die bisher verwendeten Musterklauseln entsprachen nicht mehr den gesetzlichen Anforderungen.

In langwierigen Verhandlungen haben sich die Datenschutzaufsichtsbehörden und der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) gemeinsam bemüht, die Einwilligungs- und Schweigepflichtentbindungserklärungen gesetzeskonform und transparenter zu gestalten. Der Düsseldorfer Kreis als Zusammenschluss der deutschen Datenschutzaufsichtsbehörden hat die neue Mustererklärung mit Beschluss vom 17. Januar 2012 (**Anlage 30**) gebilligt und veröffentlicht. Sie wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft.

Gemäß § 38a BDSG können sich nämlich Berufsverbände Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen geben, und der GDV hat als erster Verband davon Gebrauch gemacht.

Nach weiteren Verhandlungen mit der AG Versicherungswirtschaft des Düsseldorfer Kreises sind die Verhaltensregeln schließlich vom örtlich zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit anerkannt worden.

Versicherungsunternehmen, die diesen Verhaltensregeln beitreten, zeigen sich datenschutzfreundlich und dokumentieren damit u. a., dass sie ein umfassendes Datenschutz- und Datensicherheitskonzept vorzuweisen

haben und ihre Kunden über alle wichtigen Aspekte ihrer Datenverarbeitung informieren wollen. Beigetretene Versicherungsunternehmen sollen auf der Webseite des GDV veröffentlicht werden.

Auch der Landesbeauftragte hält solche, von den Aufsichtsbehörden geprüfte Selbstverpflichtungen für einen sinnvollen Weg, die allgemeinen Bestimmungen des Datenschutzrechts branchentypisch umzusetzen.

Das Bundesverfassungsgericht hat erneut die Bedeutung des Datenschutzes im privaten Versicherungsrecht im Hinblick auf staatliche Schutzpflichten bekräftigt. Zur Begründung hat es auf das Machtungleichgewicht zwischen den Versicherungsgebern und den Versicherungsnehmern verwiesen (Beschluss vom 17. Juli 2013, 1 BvR 3167/08; vgl. Beschluss vom 23. Oktober 2006, 1 BvR 2027/02).

13.4 Werbewirtschaft

13.4.1 Benachrichtigung der Betroffenen

Vereinzelt erreichten den Landesbeauftragten Anrufe besorgter Bürger, denen zuvor durch Unternehmen schriftlich mitgeteilt worden war, dass ihre personenbezogenen Daten (erstmalig) gespeichert oder übermittelt worden sind. Diese Sorgen waren unbegründet, denn diese Verfahrensweise entspricht prinzipiell der Rechtslage.

Gemäß § 33 Abs. 1 BDSG ist der Betroffene grundsätzlich von der erstmaligen Speicherung oder Übermittlung seiner personenbezogenen Daten zu benachrichtigen.

Insbesondere für Unternehmen der Werbebranche, Auskunfteien, Adresshändler gilt: *„Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.“*

Andere Unternehmen, private Personen oder Stellen haben sich hiernach zu richten: *„Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen.“*

13.4.2 E-Mail-Newsletter einer Versandapotheke

Eine überregional bekannte Versandapotheke in Sachsen-Anhalt wollte ihre Kunden regelmäßig informieren und versendete ungefragt per E-Mail Newsletter. Ungefragt heißt in diesem Fall: Ohne die erforderliche Einwilligung der Kunden. Damit konfrontiert, trug die Apotheke vor, es habe technische Probleme gegeben. Diese Argumentation hat der Landesbeauftragte in diesem konkreten Einzelfall jedoch für eine bloße Schutzbehauptung gehalten.

Er weist ausdrücklich alle Unternehmen, die werben wollen, darauf hin, dass bei Werbung unter Verwendung elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt, i. d. R. eine unzumutbare Belästigung anzunehmen ist (§ 7 Abs. 2 Nr. 3 UWG) und ein Bußgeldtatbestand nach dem Bundesdatenschutzgesetz erfüllt sein kann.

Auch außerhalb des E-Mail-Verkehrs ist Werbung nur in eingeschränkten Fällen zulässig. Regelmäßig ist dazu gemäß § 28 Abs. 3 Satz 1 BDSG eine schriftliche Einwilligung erforderlich. Ausnahmen davon gelten nur in den in § 28 Abs. 3 Satz 2 BDSG benannten Fällen (z. B. bei Werbung für eigene Angebote). Ist auch diese Werbung unerwünscht, hilft der Widerspruch nach § 28 Abs. 4 BDSG.

13.5 Datenschutz im Verein

Immer wieder wenden sich Mitglieder, aber auch datenschutzbewusste Vorsitzende, an den Landesbeauftragten und wollen wissen, was beim Umgang mit personenbezogenen Daten im Verein geht – und was nicht.

Typischerweise werden in jedem Verein personenbezogene Daten (zumindest der Mitglieder) erhoben, gespeichert, übermittelt und genutzt. Jeglicher Umgang mit personenbezogenen Daten unterliegt jedoch dem sog. Verbot mit Erlaubnisvorbehalt. Dieses ist in § 4 Abs. 1 BDSG geregelt. Danach sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Eine solche Erlaubnis findet sich in der Vorschrift des § 28 Abs. 1 Nr. 1 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung der Mitgliedschaft mit dem Betroffenen (Mitglied) erforderlich ist.

Auf dieser Grundlage dürfen allerdings nur die Daten erhoben, verarbeitet und genutzt werden, die für die Vereinsmitgliedschaft unbedingt erforderlich sind (z. B. Name, Anschrift, Geburtsdatum, ggf. Sportart).

Darüber hinaus kann der Umgang mit personenbezogenen Daten zulässig sein, wenn das Mitglied eingewilligt hat. Damit eine Einwilligung allerdings wirksam ist, muss sie den Anforderungen des § 4a BDSG genügen. Danach ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Mitglieds beruht. Das Mitglied ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie ggf. auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf grundsätzlich der Schriftform. Zudem ist zu beachten, dass jede Einwilligung jederzeit (mit Wirkung für die Zukunft) widerrufen werden kann.

Folgende Fallgestaltungen sind für die Praxis häufig relevant:

Mitteilungen in Aushängen

In vielen Vereinen ist es gängige Praxis, personenbezogene Informationen am Schwarzen Brett auszuhängen oder in Vereinsblättern bekannt zu geben. Informationen, die in engem Zusammenhang mit dem (Sport-)Verein stehen; z. B. die Bekanntgabe von Spielaufstellungen, Turniersiegern o. ä. sind grundsätzlich zulässig, wenn die Bekanntgabe nicht über Name und Geburtsjahr bzw. Altersklasse hinausgeht. Bei der Veröffentlichung von Vereinsjubiläen von Mitgliedern oder dem Beitritt neuer Mitglieder empfiehlt es sich aber, die Einwilligung der Mitglieder generell (bei Eintritt in den Verein) oder im Einzelfall einzuholen. Datenschutzrechtlich problematisch ist stets die Mitteilung von Daten aus dem persönlichen Lebensbereich der Mitglieder, beispielsweise Eheschließungen, Abschluss von Schul- oder Berufsausbildungen. Hierfür ist grundsätzlich die Einwilligung der betroffenen Mitglieder erforderlich.

Veröffentlichungen im Internet

Mit der Veröffentlichung im Internet geht eine potentielle Datenübermittlung auch in das Ausland einher, weil die veröffentlichten personenbezogenen Daten weltweit abgerufen werden können. Deshalb ist vor der Veröffentlichung sorgfältig zu überlegen, welche personenbezogenen Informationen im Internet wirklich unbedingt notwendig sind.

Aus Gründen der Rechtssicherheit und Transparenz ist hier die vorherige Einholung schriftlicher Einwilligungserklärungen geboten. Altmitglieder können mit einer allgemeinen Information in den Vereinsmitteilungen, einer Zustimmungserklärung und dem Hinweis auf das jederzeitige Widerrufsrecht erreicht werden. Bei Neumitgliedern empfiehlt es sich, bereits bei Vereinseintritt die Einwilligung in die Weitergabe ihrer personenbezogenen Daten einzuholen.

In Bezug auf zur Veröffentlichung vorgesehene Fotos ist auch das Kunsturheberrechtsgesetz (KunstUrhG) zu beachten. Dieses regelt das Recht am eigenen Bild als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts. Nach § 22 Satz 1 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Eine konkludente Einwilligung in die Verbreitung ist möglich. Das gilt z. B., dann wenn der Abgebildete eine Entlohnung erhalten hat (§ 22 Satz 2 KunstUrhG). Das Erfordernis der Einwilligung entfällt, wenn die abgebildete Person Beiwerk neben einer Landschaft oder einer sonstigen Örtlichkeit ist (§ 23 Abs. 1 Nr. 2 KunstUrhG).

13.6 Verkehr

13.6.1 VEMAGS-Staatsvertrag – Fehlanzeige

Hinter der Bezeichnung VEMAGS (Verfahrensmanagement für Großraum- und Schwertransporte) steht das internetbasierte Online-Genehmigungs-

verfahren für Großraum- und Schwertransporte (VEMAGS-Verfahrens-Modul) als eines von vier Modulen des Gesamt-Systems VEMAGS. Die Entwicklung und Einführung des VEMAGS-Verfahrens-Moduls, als eines der wichtigsten Projekte der damaligen E-Government-Initiative „Deutschland-Online“, stand unter der Federführung des Landes Hessen. Der Pilotbetrieb des VEMAGS-Verfahrens-Moduls erfolgte im August 2007. Seit 2008 wird das Verfahren flächendeckend in allen Ländern genutzt und steht damit den Antragstellern von Groß- und Schwerlasttransporten bundesweit zur Verfügung. Es ersetzt damit das bisherige schriftliche bzw. per Telefax notwendige Antragsverfahren zur Erlaubnis gem. § 29 Abs. 3 StVO bzw. zur Ausnahmegenehmigung gem. § 46 Abs. 1 Nr. 2 und Nr. 5 StVO für Großraum- bzw. Schwertransporte. Lange Bearbeitungszeiten, Verzögerungen im Informationsfluss zwischen Antragstellern und Genehmigungsbehörden sowie mit weiteren anzuhörenden Behörden und hohe Kosten im herkömmlichen papier- und faxgebundenen Antragsverfahren gaben damals den Ausschlag für dieses E-Government-Projekt und dessen bundesweite Einführung. Der technische Betrieb des VEMAGS-Verfahrens-Moduls erfolgt durch ein beauftragtes privates Unternehmen.

Das VEMAGS-Verfahrens-Modul bildet dabei sämtliche Schritte von der Antragstellung, dem Status der Bearbeitung bis zur Bescheidzustellung aktuell und komplett elektronisch über eine zentrale Datenbank ab, auf die über das Internet durch alle registrierten Beteiligten zugegriffen werden kann. Im Ergebnis erhält der Antragsteller einen digitalen, bundesweit einheitlichen Genehmigungsbescheid, der auch den im Verfahren registrierten Polizeibehörden der Länder als Kontrollbehörden zur Verfügung steht.

Schon frühzeitig wurde seitens der Datenschutzbeauftragten des Bundes und der Länder auf die erforderliche Schaffung einer gesetzlichen Grundlage für dieses länderübergreifende, internetbasierte Verfahren mittels einer zentralen Verbunddatei durch Gesetz oder Staatsvertrag hingewiesen. Gerade durch die zentrale Speicherung und den Zugriff der verschiedenen Nutzer auf die im System gespeicherten Daten konnte von einer bloßen Änderung des Antragsverfahrens vom Papier in die elektronische Form nicht die Rede sein. Die Einführung des Testbetriebes des VEMAGS-Verfahrens-Moduls erfolgte auf Basis einer Verwaltungsvereinbarung für den vorläufigen Betrieb zwischen den Ländern, der der Bund beigetreten war. Allerdings blieben die Bemühungen des Hessischen Ministeriums für Wirtschaft, Verkehr und Landesentwicklung mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder zur Schaffung einer solchen Rechtsgrundlage im StVG bzw. der StVO durch das dafür zuständige Bundesministerium für Verkehr, Bau und Stadtentwicklung erfolglos. Die Forderung nach einer gesetzlichen Grundlage wurde mit dem Übergang vom Testbetrieb zum ständigen Regelbetrieb im Jahr 2012 immer dringlicher.

Den Landesbeauftragten erreichte im August 2012 die Bitte des Landesministeriums für Landesentwicklung und Verkehr, zum Entwurf eines Staatsvertrages für dieses gemeinsame E-Government-Verfahren der Länder VEMAGS Stellung zu nehmen. Der Landesbeauftragte kam zum Ergebnis, dass der Entwurf, insbesondere in Artikel 9 (Datenschutz), die

Komplexität der dabei beteiligten Stellen und die unterschiedlichen anzuwendenden Rechtsvorschriften datenschutzrechtlich in diesem länderübergreifenden Informationssystem nicht hinreichend abbildete. Auch eine geplante Speicherdauer von acht Jahren nach Bescheiderstellung war aus datenschutzrechtlicher Sicht nicht nachvollziehbar. Abschließend wies der Landesbeauftragte darauf hin, dass der Artikel 12 Abs. 4 des Entwurfs erklärungsbedürftig war, nach dem dieser Staatsvertrag nach Beschlussfassung über einen endgültigen technischen Betrieb des Gesamt-Systems VEMAGS außer Kraft treten sollte und sich so damit die Frage nach einer Rechtsgrundlage wieder neu stellen würde.

Auch wenn gem. Artikel 91c Abs. 3 GG die Länder den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren können, kann dies nur erfolgen, wenn eine entsprechende Rechtsgrundlage dies ermöglicht.

Auf Nachfrage des Landesbeauftragten teilte das Ministerium für Landesentwicklung und Verkehr mit, dass der Entwurf weiter in den jeweiligen Fachgremien beraten wurde, bisher aber kein Staatsvertrag zu Stande gekommen sei. Der Landesbeauftragte soll zum Verfahrensstand weiter informiert werden.

13.6.2 Schwarzfahrerdatei beim ÖPNV

Bei Fahrkartenkontrollen wird immer wieder festgestellt, dass Fahrgäste über keine oder keine gültige Fahrkarte verfügen. Die als Schwarzfahrer bezeichneten Fahrgäste haben nach den Beförderungsbedingungen der Verkehrsunternehmen ein erhöhtes Beförderungsentgelt (EBE) zu zahlen. Zahlt der Schwarzfahrer das EBE sofort, sollte die Angelegenheit erledigt sein. Interessanter, vor allem aus datenschutzrechtlicher Sicht, sind die Fälle, in denen die Schwarzfahrer das EBE nicht sofort entrichten. Von diesen werden die zur Identifizierung erforderlichen personenbezogenen Daten erhoben und vom Verkehrsunternehmen gespeichert. Erhoben werden neben Angaben zum benutzten Verkehrsmittel, Name und Vorname des Betroffenen, seine Adresse und sein Geburtsdatum (bis zur Kontrolle durch den Landesbeauftragten wurde auch sein Geburtsort erfasst; davon soll zukünftig Abstand genommen werden). Die Daten werden gespeichert, um den Zahlungseingang des EBE überwachen zu können und bei Ausbleiben der Zahlung das Mahnverfahren (§ 688 ZPO) durchführen oder auch Strafantrag wegen Beförderungserschleichung (§ 265a Abs. 3 StGB i. V. m. §§ 247, 248a StGB) stellen zu können. Als Rechtsgrundlage dient § 28 BDSG, der die Datenerhebung und -speicherung für eigene Geschäftszwecke regelt.

Die Datenspeicherung hat der Landesbeauftragte aufgrund einer Beschwerde bei einem Verkehrsunternehmen kontrolliert. Es bestand Grund zu der Annahme, dass die Daten über einen langen Zeitraum vorgehalten wurden. Bei der Speicherung unterschied das Unternehmen zwischen kostenlos zu befördernden Kindern (unter 6 Jahre), Schuldunfähigen (unter 14 Jahre) und Minderjährigen (unter 18 Jahre). Von Kindern werden erwartungsgemäß keine personenbezogenen Daten erhoben. Bei Schuld-

unfähigen sieht das Unternehmen von einem Strafantrag ab, da selbst Wiederholungsfälle nicht als Beförderungserschleichung nach § 265a StGB verfolgt werden können. Datenschutzrechtlich problematisch war die Behandlung der Fälle, in denen die Schwarzfahrer 14 Jahre oder älter waren, wobei zwischen 14- bis 17-jährigen und volljährigen Personen (§ 2 BGB) zu unterscheiden war. Bei den 14- bis 17-jährigen wurden zusätzlich noch die Daten der Erziehungsberechtigten erhoben und gespeichert.

Über die Frage der Speicherdauer und den Zweck der vorgefundenen fortgesetzten Speicherung der Schwarzfahrerdaten bestand jedoch kein Konsens zwischen dem Landesbeauftragten und dem Verkehrsunternehmen.

Zunächst ist festzustellen, dass in den Fällen, in denen das EBE nachträglich und fristgerecht gezahlt worden ist und keine weiteren Schritte gegen den Betroffenen unternommen werden, keine Zahlungsansprüche des Unternehmens gegen diesen Betroffenen mehr bestehen und damit ein rechtsgeschäftliches Schuldverhältnis im Sinne von § 28 BDSG mit dem Betroffenen nicht mehr besteht. Eine Datenspeicherung zur Durchsetzung noch bestehender Ansprüche gegen den Betroffenen oder für die Erfüllung eigener Geschäftszwecke des Unternehmens scheidet damit in diesen Fällen aus. Zu hinterfragen wären nur mögliche Folgen von Wiederholungstaten. Das Tarifrecht und die Beförderungsbestimmungen sehen eine Erhöhung des EBE im Wiederholungsfall nicht vor.

Für die Staatsanwaltschaft sei, so erfuhr der Landesbeauftragte, im Fall des Stellens eines Strafantrages überhaupt nicht von Interesse, ob ein Wiederholungsfall vorliege. Im Übrigen werde, so das Verkehrsunternehmen, Strafantrag ohnehin nur gestellt, wenn offene uneinbringliche Forderungen gegen den Betroffenen vorlägen. Damit gilt für Fahrgäste, die ohne gültigen Fahrausweis angetroffen wurden und das geltend gemachte EBE zahlten, dass mangels Rechtsgrundlage und mangels Erforderlichkeit die Speicherung ihrer personenbezogenen Daten ab dem Zeitpunkt zu unterbleiben hat, an dem der Eingang des EBE buchungstechnisch realisiert und abgeschlossen worden ist.

Der Landesbeauftragte hatte sich mit dem Unternehmen darauf verständigt, dass eine Speicherung der Schwarzfahrer mit Blick auf die Antragsfrist gem. § 77b Abs. 1 StGB nur für die Dauer von 3 Monaten erforderlich sei.

Interessanterweise fühlte sich das Unternehmen kurz danach an diese Vereinbarung nicht mehr gebunden. Das Zeitfenster zur Erkennung von Wiederholungstätern belief sich nun auf 2 Jahre. Dies begründete das Unternehmen damit, dass EBE-Fälle länger gespeichert werden müssen. Bezug genommen wurde dabei auf die Berliner Verkehrsbetriebe, bei denen EBE-Fälle auch für 2 Jahre gespeichert würden. Allerdings ergab eine Analyse der Berliner Rechtslage interessante Unterschiede:

Davon abgesehen, dass die Berliner Verkehrsbetriebe als Anstalt des öffentlichen Rechts organisiert sind, während das kontrollierte Unternehmen

in der Rechtsform einer GmbH aufgestellt ist, hat der Berliner Gesetzgeber offenbar im Personenbeförderungsgesetz, in der Verordnung über die allgemeinen Beförderungsbedingungen für den Straßenbahn- und O-Busverkehr sowie den Linienverkehr mit Kraftfahrzeugen und im Bundesdatenschutzgesetz keine ausreichenden Rechtsgrundlage für die Speicherung von EBE-Fällen für die Dauer von 2 Jahren gesehen. Er hat deshalb eine eigene Rechtsgrundlage geschaffen. Dies ist die aufgrund des Berliner Betriebegesetzes erlassene „Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Stadtreinigungsbetrieben (BSR), den Berliner Verkehrsbetrieben (BVG) und den Berliner Wasserbetrieben (BWB) vom 30. Juni 1994“. Eine vergleichbare Regelung existiert in Sachsen-Anhalt nicht. Deshalb ist die Rechtslage nicht auf Sachsen-Anhalt übertragbar.

Im Juli 2012 hat der Landesbeauftragte das für den ÖPNV zuständige Ministerium für Landesentwicklung und Verkehr um Stellungnahme gebeten, welche auf der derzeitigen Rechtsgrundlage beruhende maximale Speicherfrist für erledigte EBE-Vorfälle es für die in Sachsen-Anhalt ansässigen Verkehrsunternehmen sieht, welche Speicherfrist es unter gleichmäßiger Berücksichtigung der Interessen der Verkehrsunternehmen und der betroffenen Fahrgäste für angemessen halten würde und ob es unter Umständen in Bezug auf eine angemessene Speicherfrist Handlungsbedarf beim Bundes- oder Landesgesetzgeber sieht.

Mit erheblicher Verzögerung, nämlich erst Ende Juni 2013, äußerte sich das Ministerium. Es war der Meinung, dass das Speichern der personenbezogenen Daten der Schwarzfahrer möglich sei, da eine Beeinträchtigung der schutzwürdigen Interessen dieser Betroffenen zu verneinen sei. Bei vertragswidrigem und strafrechtlich relevantem Verhalten bestehe kein besonderer Schutz.

Diese Argumentation hält der Landesbeauftragte für rechtlich bedenklich, da nach Ablauf der dreimonatigen Antragsfrist eine Strafverfolgung grundsätzlich nicht mehr möglich ist. Diese Praxis des Verkehrsunternehmens kommt einer Vorratsdatenspeicherung gleich.

Unklar ist auch, wie mit den Fällen umgegangen wird, in denen der Fahrgast das Bestehen eines EBE-Anspruchs bestreitet, weil er z. B. aufgrund eines Organisationsverschuldens des Unternehmens keine Fahrkarte lösen konnte. Hier besteht ein berechtigtes Interesse des Fahrgastes, nicht in die Schwarzfahrerdatei aufgenommen zu werden.

Vor diesem Hintergrund dürfte die Praxis rechtswidrig sein, so dass weiterer Klärungsbedarf besteht.

13.6.3 Fahrgastzählung im ÖPNV

Schwerbehinderte Menschen, die infolge ihrer Behinderung in ihrer Bewegungsfähigkeit im Straßenverkehr erheblich beeinträchtigt oder hilflos oder gehörlos sind, werden nach § 145 Abs. 1 SGB IX von Unternehmen, die öffentlichen Personenverkehr betreiben, unentgeltlich befördert. Das dient

dazu, ihre Selbständigkeit und gleichberechtigte Teilhabe am Leben in der Gesellschaft zu fördern. Dafür steht den Verkehrsunternehmen eine angemessene Erstattung der entstehenden Fahrgeldausfälle zu. In Sachsen-Anhalt ist das Landesverwaltungsamt die Erstattungsbehörde. Die Erstattung erfolgt auf Basis eines von der Landesregierung ermittelten Prozentsatzes der schwerbehinderten Menschen an der Wohnbevölkerung in Sachsen-Anhalt. Das anzuwendende mathematische Verfahren wird in § 148 Abs. 4 SGB IX beschrieben. Der Gesetzgeber hat auch für den Fall vorgesorgt, dass im Bereich eines Verkehrsunternehmens wesentlich mehr schwerbehinderte Menschen leben und von ihm befördert werden müssen, als sich aus dem beschriebenen Standardverfahren ergibt. Das Verkehrsunternehmen kann nach § 148 Abs. 5 SGB IX durch Verkehrszählung nachweisen, dass das Verhältnis zwischen den unentgeltlich zu befördernden und den sonstigen Fahrgästen den im oben beschriebenen Verfahren festgesetzten Prozentsatz um mindestens ein Drittel übersteigt. In diesem Fall würde der Erstattungsbetrag entsprechend erhöht. Zur Regelung des Verfahrens hat das Ministerium für Arbeit und Soziales die „Richtlinie über die Erstattung der Fahrgeldausfälle im Nahverkehr nach § 148 SGB IX“ (MBl. LSA 2006 S. 461, geändert durch RdErl. vom 19. April 2007, MBl. LSA 2007 S. 426) erlassen. In Nr. 4 der als Durchführungsbestimmung zu verstehenden Richtlinie ist die Datenerhebung bei den Verkehrszählungen, die durch die Verkehrsunternehmen selbst oder durch Dritte in deren Auftrag durchgeführt werden, konkret geregelt. Da den Fahrgästen in vielen Fällen nicht angesehen werden kann, dass sie zur kostenlosen Inanspruchnahme der Beförderungsleistung berechtigt sind, kann eine exakte Fahrgastzählung nur durch die Kontrolle der Fahrkarten bzw. der Schwerbehindertenausweise einschließlich Beiblatt und gültiger Wertmarke erfolgen. Das Zählpersonal muss zur Fahrkartenkontrolle berechtigt sein und sich ausweisen, denn die Beförderungsbedingungen und Tarifbestimmungen legen fest, dass der Fahrgast die Fahrkarte oder den Schwerbehindertenausweis den Kontrolleuren auf Verlangen vorzuzeigen hat.

Über die Praxis dieser Kontrollen beschwerte sich ein Petent, der Inhaber eines Schwerbehindertenausweises war. In seinem Fall hatte das Kontrollpersonal keine Berechtigung zur Kenntnisnahme seiner personenbezogenen Daten besonderer Art.

Des Weiteren wurde die hier durchgeführte Zählung der kostenlos zu befördernden schwerbehinderten Menschen mit einer Fahrgastzählung nach § 8a ÖPNVG LSA verbunden. Diese Zählung soll die Ausnutzung von Zeitfahrausweisen bestimmen, denn der normale ÖPNV wird durch zweckgebundene Zuwendungen auf Basis der verkauften Fahrkarten gefördert. Auch in diesem Fall erhöht sich der Zuwendungsbetrag, wenn das Verkehrsunternehmen eine überproportionale Ausnutzung der Zeitfahrausweise gem. § 8a Abs. 1 ÖPNVG LSA nachweisen kann.

Bei der Kontrolle von Zeitfahrausweisen kommt es ebenfalls zu einer Kenntnisnahme der personenbezogenen Daten des Fahrausweisinhabers, denn sein Name und seine Adresse sind auf dem Fahrausweis aufgedruckt. Er verliert also bei einer Fahrkartenkontrolle seine Anonymität, sein

Verkehrsverhalten wird teilweise transparent, da die Zähler die Fahrgäste auch befragten, wo sie ein- und aussteigen und welchem Zweck die Fahrt dient.

Da die Berechtigung der Kontrolleure in dem beim Landesbeauftragten vorgebrachten Fall nicht vorlag, hätte die Fahrkartenkontrolle und die erweiterte Befragung der Fahrgäste allenfalls auf freiwilliger Basis erfolgen können. Darauf hätten die Fahrgäste nach § 4 Abs. 3 Satz 2 BDSG hingewiesen werden müssen. Die stattdessen verwendeten Worte „An dieser Befragung müssen Sie teilnehmen“ waren jedenfalls der Grund für den Petenten, sich beim Landesbeauftragten über die Zwangsdatenerhebung zu beschweren.

Dem Landesbeauftragten wurde von dem betroffenen Verkehrsunternehmen versichert, dass bei zukünftigen Zählungen die Fahrgäste korrekt angesprochen werden.

13.6.4 Verwarnungen auf Vorrat im ruhenden Verkehr

Bereits Ende des Jahres 2011 wurde der Landesbeauftragte durch eine Stadtverwaltung hinsichtlich der datenschutzrechtlichen Bewertung eines geplanten Modellversuchs im ruhenden Verkehr angefragt. Die Idee der Stadtverwaltung bestand darin, falsch parkende Kraftfahrer – im Blick hatte die Stadtverwaltung neben Einheimischen vor allem auswärtige Besucher der Stadt – bei einem erstmaligen Verstoß in einer Parkverbotszone mittels einer „Gelben Karte“ eine Verwarnung ohne Verwarnungsgeld auszusprechen. Diese an sich gute Idee setzt aber die Speicherung der amtlichen Kennzeichen der Falschparker voraus. Genau darin lag das datenschutzrechtliche Problem, da eine Rechtsgrundlage für diese Vorratsspeicherung der amtlichen Kennzeichen nicht gegeben ist. Bereits im Jahr 1997 hatte der Landesbeauftragte in seinem III. Tätigkeitsbericht (Nr. 29.4.) die Rechtslage und die Unzulässigkeit dieser Speicherung erläutert, denn als bereichsspezifische Regelung sind hier die §§ 28 bis 30c StVG einschlägig. Hintergrund waren damals Dateimeldungen bzw. Anfragen kommunaler Ordnungsämter zur Speicherung abgeschlossener Verwarngeldverfahren bei Verkehrsordnungswidrigkeiten im ruhenden Verkehr. Darauf hatte das damalige Ministerium des Innern mit einem Erlass vom 5. Januar 1996 reagiert und ebenfalls auf die bestehende Rechtslage hingewiesen und die Speicherung in Dateien von „Mehrfachtätern“ für unzulässig erklärt.

Im Frühjahr des Jahres 2012 erhielt der Landesbeauftragte von einem Petenten aus eben dieser Stadt eine Eingabe, in der eine Beendigung dieser rechtlich unzulässigen Praxis gefordert wurde. Daraufhin wurde der Stadt sowohl im persönlichen Gespräch als auch abschließend schriftlich die bestehende Rechtslage eingehend erläutert, auf die Unzulässigkeit der Speicherung dieser Daten hingewiesen und die Einstellung dieses Modellversuches und die Löschung der Daten angemahnt. Mit der Antwort hat sich die Stadtverwaltung allerdings viel Zeit gelassen und lediglich mitgeteilt, dass man zu einer anderen Rechtsauffassung als der Landesbeauftragte gekommen sei und an der bisherigen Praxis festhalten wolle. An-

zumerken ist noch, dass die vom Landesbeauftragten vertretene Rechtsauffassung, vom Bundesverwaltungsgericht geteilt wird (Urteil vom 17. Dezember 1976, VRS 52, 381). Der Landesbeauftragte hat deshalb der Stadt selbst eine „Gelbe Karte“ gezeigt und sie nochmals aufgefordert, eine inhaltlich begründete Stellungnahme abzugeben, die bisherige Speicherpraxis einzustellen und die gespeicherten Daten zu löschen.

Da seitens der Stadtverwaltung keine weitere inhaltliche Stellungnahme einging, wurde nun seitens des Ministeriums für Inneres und Sport, das die Rechtsauffassung des Landesbeauftragten teilt, die obere Kommunalaufsichtsbehörde, das Landesverwaltungsamt, im August 2013 angewiesen, tätig zu werden. Wenn die Stadtverwaltung doch noch einlenkt, könnte der Landesbeauftragte auf eine „Rote Karte“ in Form einer formellen Beanstandung gem. § 24 Abs. 1 DSG LSA verzichten.

Der Landesbeauftragte empfiehlt dem Ministerium für Inneres und Sport, über einen erneuten Erlass zu diesem Thema nachzudenken, denn der Erlass aus dem Jahr 1996 ist schon lange außer Kraft.

13.6.5 Besitzeinweisungsverfahren nach dem Allgemeinen Eisenbahngesetz

Zur Errichtung einer Hochspannungsleitung für ein Verkehrsunternehmen war es notwendig, Grundstücksflächen für den Bau von Strommasten in Anspruch zu nehmen und die von den Leiterseilen überspannten Flächen dinglich zu sichern, also das Recht im Grundbuch einzutragen, die Leitung zu betreiben. In einem Fall verliefen die entsprechenden mit den Grundstückseigentümern bzw. Nutzungsberechtigten geführten Kauf- bzw. Entschädigungsverhandlungen ergebnislos, sodass das Verkehrsunternehmen beim Landesverwaltungsamt den Antrag auf Besitzeinweisung stellte. Außerdem beauftragte es einen öffentlich bestellten und vereidigten Sachverständigen. Dieser sollte die Bewertung von bebauten und unbebauten Grundstücken vornehmen.

Dazu waren Aufwuchsentschädigungen zur Feststellung des Entschädigungswertes für die in Anspruch zu nehmende Grundstücksteilfläche festzustellen und der Aufwuchs zu bewerten. Diese Zustandsfeststellung war vom Sachverständigenbüro zunächst dem Verkehrsunternehmen, von diesem dem Landesverwaltungsamt und von diesem schließlich den Beteiligten bzw. Betroffenen zur Kenntnis gegeben worden. Das Verfahren wurde nach den Vorschriften des § 21 AEG geführt.

Ein Petent hat dem Landesbeauftragten gegenüber jedoch grundsätzliche Bedenken erhoben. Er bat zu prüfen, ob durch die Zuleitung der die Grundstücke und Pachtverträge betreffenden Unterlagen an alle in diesem Verfahren beteiligte Dritte die Betroffenen in ihren Rechten beeinträchtigen sein könnten.

Der Eigentümer des Flurstückes, von dem der Petent vom Landesverwaltungsamt Grundbuchauszüge und andere Unterlagen zugesandt bekam, war ein ihm nicht näher bekannter Dritter. Durch diesen war das Flurstück zur landwirtschaftlichen Nutzung an einen Landwirt verpachtet worden. Im

Wege des nach § 1 des Pachtvertrages ausdrücklich zugelassenen Pflugtausches tauschte dieser das Nutzungsrecht an der Ackerfläche gegen selbiges an einer anderen Fläche. Vertragspartner des zeitweiligen Flächentausches (Bewirtschaftungsaustausch) war der Petent, der nun erfuhr, wie hoch die Pacht des von ihm bewirtschafteten Grundstücks war und ob der Eigentümer es mit einer Hypothek belastet hatte. Die Kenntnis dieser Umstände ist jedoch nicht erforderlich. Schließlich würden in den vielen vergleichbaren Fällen, Pflugtausch sei bei den Landwirten in seinem Landkreis eher die Regel als die Ausnahme, unzulässig Unterlagen an nur sekundär Beteiligte versandt. Damit würden besonders sensible personenbezogene Daten, wie z. B. der vereinbarte Pachtpreis oder die Eintragungen in Abteilung 3 des Grundbuches, unzulässig übermittelt.

Obgleich das Verfahren der vorzeitigen Besitzeinweisung in § 21 AEG geregelt ist und nach erstem Anschein im vorliegenden Fall so verfahren worden war, bat der Landesbeauftragte das Landesverwaltungsamt um Stellungnahme. Zum Beispiel ging es darum festzustellen, ob mittelbar Betroffene – also nicht nur Eigentümer oder Pächter, sondern auch Pflugtauschpartner – Beteiligte im Sinne des Verwaltungsverfahrens sind, denen nach dem AEG und den allgemeinen verwaltungsverfahrensrechtlichen Grundsätzen die Anhörungsunterlagen und später auch der Besitzeinweisungsbeschluss insgesamt zuzustellen sind.

Das Landesverwaltungsamt teilte dem Landesbeauftragten mit, dass § 21 AEG im vorliegenden Fall keinen Ermessensspielraum ließe, da nach dem Gesetz der Eigentümer des Grundstücks, der Antragsteller auf die vorzeitige Besitzeinweisung und die Inhaber von solchen Rechten, die zum Besitz oder zur Nutzung des Grundstückes berechtigen, Verfahrensbeteiligte seien. Mit der Ladung zur mündlichen Verhandlung im vorzeitigen Besitzeinweisungsverfahren müssten, so das Landesverwaltungsamt, die Verfahrensbeteiligten darauf hingewiesen werden, dass der Antrag mit den entsprechenden Anlagen bei der Enteignungsbehörde auch eingesehen werden könnte. Das Landesverwaltungsamt sehe jedoch das datenschutzrechtliche Problem ebenso wie der Landesbeauftragte und wolle zukünftig dafür sorgen, dass solche Daten bzw. Angaben, die zur Erfüllung der Aufgabe „vorzeitige Besitzeinweisung“ nicht erforderlich seien, nicht in die Zustandsfeststellung aufgenommen würden. Dies wäre eine datenschutzrechtlich gute Lösung, wenn das Landesverwaltungsamt diese entsprechend umsetzt.

Anlagen

Nationale Datenschutzkonferenz

Anlage 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdienstean-bietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsda-

ten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

Anlage 2

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

Anlage 3

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze - gerade in ihrem Zusammenwirken - durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

Anlage 4

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,

2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,

3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,

4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und

5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

Anlage 5

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir“-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Dienstanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der

immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Anlage 6

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzende sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.

- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.

- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.

- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, sodass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

Anlage 7

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat (OH „Cloud Computing“ vom 26. September 2011).

Anlage 8

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München

Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012

Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Land eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

Anlage 10

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012 in Potsdam

Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik - insbesondere der Videoüberwachung und dem Instrument der Mustererkennung - menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

Anlage 11

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012 in Potsdam

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in

Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die

vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Anlage 12

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012 in Potsdam

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

Anlage 13

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Mai 2012

Patientenrechte müssen umfassend gestärkt werden

Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.

- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.

- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.

- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.

- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.

- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der

Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012

Orientierungshilfe zum datenschutzgerechten 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. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.

- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.

- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.

- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.

- Die Daten sollen an möglichst wenige Stellen übermittelt werden.

- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.

- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.

- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.

- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.

- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

Anlage 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012

Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.

- Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

- Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.

- Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.

- Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

- Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.

- Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.

- Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

Anlage 16

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012 in Frankfurt (Oder)

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

- Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

- Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

- Mit Blick auf die Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Anlage 17

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012 in Frankfurt (Oder)

Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

Anlage 18

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012 in Frankfurt (Oder)

Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

Anlage 19

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012 in Frankfurt (Oder)

Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

- Interface Identifier und Präfix sollten synchron gewechselt werden.

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

Anlage 20

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Januar 2013

Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen - etwa zum Konzerndatenschutz - auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.

- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.

- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.

- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.

- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

Anlage 21

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.

- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.

- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.

- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.

- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.

- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.

- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.

- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

Anlage 22

Erläuterung zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Erläuterungen zur Entschließung „Europa muss den Datenschutz stärken“

- Jedes personenbeziehbare Datum muss geschützt werden

  Nach Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie zum Beispiel IP-Adressen, Kenn-Nummern, Standortdaten ein.

- Es darf keine grundrechtsfreien Räume geben

  Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

- Einwilligungen müssen ausdrücklich erteilt werden

  Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäische Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es - auch mit Blick auf Artikel 8 Absatz 2 der Grundrechtecharta - nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern

  Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch - in Anlehnung an Artikel 8 Absatz 2 der Grundrechtecharta - das Europäische Parlament in der Entschließung

vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

- Profilbildung muss beschränkt werden

  Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte

  Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können

  Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission

  Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Artikel 16 Absatz 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

- Grundrechtsschutz braucht effektive Kontrollen

  Die Sanktionen müssen - wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat - abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

- Hoher Datenschutzstandard für ganz Europa

  Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

Anlage 23

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.

- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen beziehungsweise absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Absatz 3 BKRG festgelegt werden.

Anlage 24

Anlage zur Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“ der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.

- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.

- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.

- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.

- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

Anlage 25

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

Anlage 26

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013 in Bremerhaven

Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

Düsseldorfer Kreis

Anlage 27

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 22. und 23. November 2011

Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt.

Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist

ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.

- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.

- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

Anlage 28

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 22. und 23. November 2011

Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden

wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment“) zu erhalten.[1]

[1] vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!“ (Anlage 8)

Anlage 29

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 8. Dezember 2011

Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten - soweit keine Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne Weiteres in das eigene Angebot einbinden.

Anlage 30

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 17. Januar 2012

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen.

(Der Text der „Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung“ steht Ihnen auf der Homepage des Landesbeauftragten unter der Rubrik Konferenzen zur Verfügung.)

Anlage 31

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 18. und 19. September 2012

Near Field Communikation (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

Anlage 32

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 26. und 27. Februar 2013

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG 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.

1. Innenkameras

   Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

   Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

   Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

   Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit „Unfallkameras“, wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Anlage 33

Orientierungshilfe der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 26. und 27. Februar 2013

Orientierungshilfe für den Umgang mit Verhaltensregeln nach § 38a BDSG

Verhaltensregeln dienen dem präventiven Datenschutz und der **regulierten Selbstregulierung** der Wirtschaft. Sie sollen gute Datenschutzpraxis vorgeben und für alle Beteiligten gegenüber den gesetzlichen Regelungen unter Berücksichtigung der praktischen Gegebenheiten bestimmter Wirtschaftsbereiche und bestimmter Formen personenbezogener Datenverarbeitung mehr Rechtssicherheit vermitteln. Um dieses Ziel zu erreichen, bedarf es eines einheitlichen Verständnisses darüber, was durch derartige Verhaltensregeln erreicht und welches Verfahren dafür beschritten werden kann und soll.

A. Rechtliche Vorgaben

Für den Umgang mit datenschutzrechtlichen Verhaltensregeln (auch CoC - Code of Conduct genannt) gibt es § 38a BDSG, der die Regelung in Art. 27 der Europäischen Datenschutzrichtlinie (95/46/EG) in nationales Recht umsetzt.

Art. 27 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. Nr. L 281 vom 23/11/1995 S. 0031 - 0050) hat folgenden Wortlaut:

Verhaltensregeln

(1) Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

(2) Die Mitgliedstaaten sehen vor, dass die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können.

Die Mitgliedstaaten sehen vor, dass sich diese Stellen insbesondere davon überzeugt, dass die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Die Stelle holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint.

(3) Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang

stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, dass die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.

§ 38a BDSG hat folgenden Wortlaut:

Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Verhaltensregeln können **gesetzliche Regeln** nicht ersetzen oder verdrängen, sollen aber diese konkretisieren (Durchführung) und im Hinblick auf den Datenschutz verbessern (Förderung). Kommt es trotz positiver Überprüfung einer Aufsichtsbehörde (Anerkennung) zu einem Widerspruch zwischen gesetzlicher Regelung und Verhaltensregel, geht das Gesetz vor.

B. Bisherige Praxis

Die Regelung des § 38a BDSG stammt aus dem Jahr 2001. Seitdem wurden den Aufsichtsbehörden einige wenige Vorschläge von Verhaltensregeln vorgelegt. Ohne dass dies empirisch nachweisbar ist, mag ein Grund dafür, dass es nur so wenige waren, auch darin liegen, dass die Datenschutzaufsichtsbehörden das Wort „Förderung“ im Gesetzestext so verstehen, dass durch die Verhaltensregeln ein datenschutzrechtlicher Mehrwert im Sinne einer Steigerung des Datenschutzniveaus erreicht werden sollte. Diese Anforderung und eine unklare Situation über die Schaffung von Rechtsverbindlichkeit mag dazu geführt haben, dass das mit viel Arbeit verbundene Aufstellen von datenschutzrechtlichen Verhaltensregeln für die Wirtschaft nicht wirklich attraktiv war. Bisher wurde deshalb lediglich in einem Fall (Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft) auf entsprechenden Antrag die Vereinbarkeit mit dem geltenden Datenschutzrecht festgestellt.

Um die Voraussetzungen dafür zu schaffen, die Wirtschaft zu motivieren, sich datenschutzrechtliche Verhaltensregeln zu geben, die im Interesse aller zu mehr Rechtssicherheit führen können, haben die Aufsichtsbehörden diese Orientierungshilfe erstellt.

C. Vollzugsverständnis der Datenschutzaufsichtsbehörden

1. Wer kann der Aufsichtsbehörde Verhaltensregeln unterbreiten?

Unterbreitungsberechtigt sind nach dem Gesetzeswortlaut „Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten“. Hierzu gehören neben klassischen Berufsverbänden auch die öffentlich-rechtlich or-

ganisierten berufsständischen Kammern. Ein Berufsverband muss nicht sämtliche Unternehmen einer Sparte vertreten. Erfasst sein können auch Vereinigungen von Auftragnehmern. Nicht ausgeschlossen sind auch Konzerne als Unternehmensvereinigungen. Einzelne Unternehmen können keine Verhaltensregeln unterbreiten. In der Vereinigung müssen Stellen vertreten sein, die für personenbezogene Datenverarbeitung verantwortlich sind; hierzu gehören nicht solche, die Betroffene, Arbeitnehmer oder Verbraucher vertreten.

2. Was kann in Verhaltensregeln geregelt werden?

Verhaltensregeln können „zur Förderung der Durchführung von datenschutzrechtlichen Regelungen“ erstellt werden. Aus der Formulierung „Durchführung“ sowohl in der Richtlinie als auch im Bundesdatenschutzgesetz ergibt sich, dass es sich bei Verhaltensregeln um keine gesetzesergänzende oder gar gesetzesändernde Regelungen handeln kann, sondern lediglich um Vollzugsregelungen. Daraus folgt, dass ein über das gesetzliche Niveau hinausgehender Datenschutzstandard nicht zwingend gefordert werden kann, und dass Verhaltensregeln, die das gesetzliche Niveau absenken wollen, nicht als vereinbar mit dem Datenschutzrecht festgestellt werden können.

Konkret folgt daraus, dass durch Verhaltensregeln insbesondere unbestimmte Rechtsbegriffe, Ermessenskriterien, Musterklauseln, verfahrensrechtliche Vorkehrungen, Vorgaben für die Bearbeitung von Betroffenenrechten oder technisch organisatorische Maßnahmen festgelegt werden können.

3. Wer entscheidet über die Durchführung eines Prüfverfahrens?

Die Berufsverbände und anderen Vereinigungen entscheiden über die Durchführung eines Prüfverfahrens, indem sie den Entwurf von Verhaltensregeln der Aufsichtsbehörde vorlegen. Dadurch wird ein Verwaltungsverfahren eingeleitet, das die Berufsverbände und anderen Vereinigungen jederzeit durch Rücknahme des Antrags auf Überprüfung beenden können. Solange ein gestellter Antrag nicht zurückgenommen ist, ist die Aufsichtsbehörde zur Durchführung des Verfahrens und zum Erlass einer abschließenden Entscheidung verpflichtet. Diese Entscheidung kann bei Vorliegen der gesetzlichen Voraussetzungen ggfls. im Wege einer Verpflichtungsklage erreicht werden.

4. An welche Aufsichtsbehörde kann sich ein Antragsteller wenden?

Soweit von dem Antragsteller Verhaltensregeln mit bundesweiter Anerkennung gewünscht werden, wird das Verfahren durch die Aufsichtsbehörde des Landes betrieben, in dem der Berufsverband oder die Vereinigung den Hauptsitz hat. Die Aufsichtsbehörden stimmen sich untereinander ab, um die bundesweite Bindungswirkung zu gewährleisten.

5. Was prüft die Aufsichtsbehörde?

Voraussetzung für die Anerkennung ist, dass die Verhaltensregeln „den Datenschutz fördern“. Nicht anerkennungsfähig sind Regeln, die die gesetzlichen Vorgaben nur abbilden oder hinter diesen zurückbleiben. Die Regeln sollten einen datenschutzrechtlichen und branchenbezogenen Mehrwert enthalten, da ein entsprechender Ko-

dex anderenfalls auf die bloße Wiederholung oder sinngemäße Wiedergabe des Gesetzestextes gerichtet wäre. Dieser Mehrwert kann in einer bereichsspezifischen Präzisierung, ergänzenden konkretisierenden Regelungen und Anforderungen, fördernden Verfahren oder Standardisierungen und technischen Festlegungen liegen.

Gegebenenfalls mag man zur Auslegung des Begriffs „Förderung“ auch auf das Verständnis der Art. 29-Datenschutzgruppe zur Auslegung von länderübergreifenden Verhaltensregeln (Art. 27 Abs. 3 RL 95/46/EG) zurückgreifen, in denen ausgeführt wird[2], dass die unterbreiteten Verhaltensregeln ausreichende Qualität und Kohärenz aufweisen und genügenden zusätzlichen Nutzen für die Richtlinien und andere geltende Datenschutzrechtsvorschriften liefern, insbesondere, ob der Entwurf der Verhaltensregeln ausreichend auf die spezifischen Fragen und Probleme des Datenschutzes in der Organisation oder dem Sektor ausgerichtet ist, für die er gelten soll, und für diese Fragen und Probleme ausreichend klare Lösungen bietet.

Ein konkretes Beispiel zur Bestimmung des branchenbezogenen Mehrwerts findet sich in einer Stellungnahme der Art. 29-Datenschutzgruppe zum europäischen Verhaltenskodex von FEDMA zur Verwendung personenbezogener Daten im Direktmarketing[3].

Zur Erhöhung der Qualität und der Akzeptanz der Verhaltensregeln kann es sinnvoll sein, die Entwürfe mit möglicherweise betroffenen Interessenvertretungen, z. B. Verbraucherschutzorganisationen, zu erörtern.

6. Wie kann das Ergebnis der Prüfung der Aufsichtsbehörde aussehen?

Ziel der Überprüfung nach § 38a Abs. 2 BDSG ist die Feststellung der Rechtskonformität der Verhaltensregeln und deren Geeignetheit „zur Förderung von datenschutzrechtlichen Regelungen“. Die Feststellung hat Regelungscharakter, ist ein feststellender, begünstigender Verwaltungsakt und kann als Anerkennung bezeichnet werden. Die Regelung liegt in der mit der Anerkennung verbundenen Verbindlichkeitserklärung, mit der eine Selbstbindung der Aufsichtsbehörde verbunden ist.

Der Regelungsbereich muss nicht, kann aber einen gesamten Wirtschaftsbereich umfassen. Regelungsfähig sind auch spezifische Rechtsfragen oder spezifische personenbezogene Anwendungen, Verfahren oder auch nur Verfahrensteile.

7. Wie können Berufsverbände und andere Vereinigungen dagegen vorgehen, wenn die zuständige Aufsichtsbehörde zu einer Unvereinbarkeit der Verhaltensregeln mit dem geltenden Datenschutzgesetz kommt?

Aus der Tatsache, dass eine Anerkennung im o. g. Sinn als feststellender begünstigender Verwaltungsakt zu qualifizieren ist, folgt, dass auch die Entscheidung der Aufsichtsbehörde, dass vorgelegte Verhaltensregeln mit dem geltenden Datenschutzrecht nicht vereinbar sind, einen feststellenden Verwaltungsakt darstellen, ge-

[2] WP 13 vom 10.09.1998,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf#h2-15

[3] Art. 29 Gruppe, WP 77;
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_de.pdf#h2-15

gen den der Antrag stellende Berufsverband oder die andere Vereinigung Rechtsschutz vor dem Verwaltungsgericht suchen kann.

8. Für welchen Bereich und wie lange gelten die Verhaltensregeln?

Der Geltungsbereich von Verhaltensregeln kann sich nur auf den nicht-öffentlichen Bereich (§§ 27 ff. BDSG) beschränken. Hinsichtlich des Adressatenkreises ist der Berufsverband oder die Vereinigung frei in der Normierung. Möglich ist – wenn das nach den eigenen Regelungen vorgesehen ist – sowohl eine automatische Verbindlichkeit für sämtliche Mitglieder oder Angehörigen wie auch eine Verbindlichkeit erst nach Beitritt eines Unternehmens.

Im Interesse größtmöglicher Transparenz und Verbindlichkeit sollte der zuständige Berufsverband oder die entsprechende Vereinigung angehalten werden, ihre Verhaltensregeln und die Feststellungsentscheidung der Aufsichtsbehörde zu veröffentlichen. Besondere rechtliche Vorgaben oder Verpflichtungen zur Veröffentlichung bestehen jedoch nicht.

Die Verbindlichkeit von anerkannten Verhaltensregeln gilt grundsätzlich auf unbestimmte Zeit, solange die Regeln nicht geändert werden. Sinnvoll ist es, Verhaltensregeln nach einer gewissen Periode zu evaluieren. An der Evaluierung können sich Aufsichtsbehörden beteiligen. Werden Verhaltensregeln geändert, was die Berufsverbände und anderen Vereinigungen jederzeit machen können, bedarf es für eine erneute Rechtsverbindlichkeit einer erneuten Antragstellung bei der Aufsichtsbehörde und des Erlasses eines entsprechenden Feststellungsbescheides.

Europäische Datenschutzkonferenz

Anlage 34

Europäische Datenschutzkonferenz vom 3. bis 4. Mai 2012 in Luxemburg

Beschluss zur Europäischen Datenschutz-Reform

– Übersetzung –

Die Frühjahrskonferenz 2012 der europäischen Datenschutzbeauftragten (130 Delegierte aus 38 Ländern), welche sich vom 3. bis 4. Mai 2012 in Luxemburg traf, erörterte die jüngsten Entwicklungen für die Modernisierung der datenschutzrechtlichen Rahmenbedingungen der EU, dem Europarat und der OECD. Die Konferenz erkannte die derzeitigen Bemühungen, den Bürgern und Verbrauchern verbesserte Rechte und effektive Wege für deren Inanspruchnahme, unter Berücksichtigung technologischer Veränderungen und der Globalisierung, zu garantieren. Die Datenschutzbeauftragten begrüßen insbesondere folgende Hauptziele:

- Die Stärkung und Präzisierung der Rechte des Einzelnen;
- Die Betonung der Verantwortung der für die Datenverarbeitung Verantwortlichen und der Datenverarbeiter;
- Die Verringerung von einigen Verwaltungslasten und der Suche nach Konsistenz;
- Die den unabhängigen Datenschutzbehörden gewidmete Schlüsselrolle;
- Der Schritt, einen umfassenderen Rahmen, der die Anwendung der grundlegenden Datenschutzprinzipien in allen Bereichen sicher stellt, zu entwickeln;
- Die Initiative des Europarats, das Übereinkommen Nr. 108, welches seit 1981 den Weg bestimmte, zu verbessern, einschließlich des Ziels, die Konsistenz und Kompatibilität mit dem Rechtsrahmen der EU zu gewährleisten und die feste Unterstützung der Absicht, genauer die Umsetzung der Konvention durch die Vertragsstaaten zu verfolgen;
- Der laufende Reflexionsprozess auf der Ebene der OECD über die Entwicklung der internationalen Privatsphären-Landschaft.

Die Konferenz analysierte auch die geplante Verbesserung der europäischen Rechtstexte vor dem Hintergrund der internationalen Entwicklungen auf dem Gebiet der Datenverarbeitung und Privatsphäre, auch in den transatlantischen Beziehungen, insbesondere im Hinblick auf das am 23. Februar 2012 veröffentlichte Überblickspapier der US-Regierung und den im März 2012 veröffentlichten Bericht der Federal Trade Commission.

Unter Berücksichtigung der zuvor angenommenen Entschließungen[4], untersuchte die Konferenz im Detail das jüngste Gesetzespaket der Europäischen Kommission zur Modernisierung der EU-Datenschutzvorschriften. Die Konferenz begrüßt, dass die Vorschläge die neuen Herausforderungen, die sich aus der allgegenwärtigen Erhebung und Nutzung von personenbezogenen Daten in einer vernetzten und globalisierten Welt ergeben, adressieren. Die Datenschutzbeauftragten sind besonders zufrieden mit:

- Die Vorschriften für mehr Transparenz und mehr Kontrolle über die Datenverarbeitung;

- Die Kodifizierung des Grundsatzes der Datensparsamkeit;

- Mehr Möglichkeiten der Wiedergutmachung für die Betroffenen;

- Die Stärkung der Vorschriften über die Rechte auf Zugang und zu widersprechen;

- Die Einbeziehung von Rechten, um die Herausforderungen, die sich aus der Online-Umgebung (ein spezifischer Schutz von Kindern, das „Recht, vergessen zu werden“ und das neue Recht auf Portabilität von Daten) ergeben, anzugehen;

- Der Versuch, vereinfachte und einheitliche Regeln für Datenverarbeitungs-Verantwortliche einzuführen;

- Die Einführung des Grundsatzes der Rechenschaftspflicht;

- Die Einführung von Mechanismen und Werkzeugen, die als Anreize zur Demonstration der Zurechenbarkeit dienen, wie Datenschutz By Design (datenschutzgerechte Produkte) und Datenschutz By Default (datenschutzgerechte Einstellungen als Vorgabe), Privatsphäre-Folgenabschätzungen, die Ernennung von Datenschutzbeauftragten und Datenpannen-Meldepflichten;

- Die Einführung einer One-Stop-Shop-Lösung sowohl für Verantwortliche, durch Erstellung des Konzepts der federführenden Behörde, welche mit anderen betroffenen Datenschutzbehörden zusammenarbeitet, als auch für Einzelpersonen (Gegenstand für letztere wird weiter verbessert);

- Das Erfordernis einer aktiven Zusammenarbeit zwischen Datenschutzbehörden und der Stärkung ihrer Unabhängigkeit und Befugnisse, einschließlich der Einführung von Bußgeldern.

Die Datenschutzbeauftragten sind überzeugt, dass das Know-how und die praktische Erfahrung der Datenschutzbehörden eine wichtige Rolle in der praktischen Anwendung der Datenschutzrechte auch in Zukunft, insbesondere durch:

---

[4] Beschluss über die Notwendigkeit eines umfassenden Rahmens für den Datenschutz, angenommen von der Europäischen Datenschutzkonferenz vom 5. April 2011 in Brüssel und Beschluss über die künftige Entwicklung des Datenschutzes und der Privatsphäre, angenommen von der Europäischen Datenschutzkonferenz vom 30. April 2010 in Prag.

1. die obligatorische Konsultation der Datenschutzbehörden bei legislativen Maßnahmen auf EU- sowie auf nationaler Ebene;

2. die Entwicklung von Leitlinien und Empfehlungen für die praktische Umsetzung, unter Berücksichtigung nationaler und sektoraler Besonderheiten;

3. die Möglichkeit zur Durchführung von Untersuchungen und Audits von Amts wegen („ex officio“)

spielen kann.

Sie wiesen auch darauf hin, dass eine gute Leistung von diesen und anderen Aufgaben, einschließlich der internationalen Zusammenarbeit in der EU und darüber hinaus, von der anhaltenden Verfügbarkeit von ausreichenden finanziellen, technischen und personellen Ressourcen abhängt.

Im Hinblick auf die Konsistenz des EU-Pakets, warnt die Konferenz vor dem Risiko, dass zu viele Ausnahmen und Abweichungen die effektive Anwendung der Hauptprinzipien des Datenschutzes verhindern. Ausnahmen, vorgesehen für Behörden, Strafverfolgung oder die Verwendung von Daten für staatliche Zwecke, einschließlich für steuerliche Zwecke, müssen mit den zentralen Aspekten des Datenschutzrechts im Einklang stehen. Wesentliche Datenschutzvorschriften sollten in konsistenter Weise und unabhängig von der jeweiligen Branche angewandt werden.

Die Konferenz stellt deshalb fest, dass weitere Verbesserungen an den aktuellen Vorschlägen erforderlich sind, insbesondere, um die vorgeschlagene Richtlinie über den Bereich der Polizei und Justiz mehr in Einklang mit den Grundprinzipien der Datenschutz-Grundverordnung bringen. Regeln bspw. zur Übertragung von Daten zwischen privaten Parteien und Strafverfolgungsbehörden, werden immer noch vermisst. Vor diesem Hintergrund sind die Datenschutzbeauftragten bereit, aktiv zum Erfolg eines modernisierten und wirksamen Datenschutz-Rahmens für Europa beizutragen.

Die Stärkung und Vereinfachung des Datenschutzes ist wichtiger als je zuvor. Die Konferenz fordert deshalb sowohl den Europarat, die ehrgeizige Revision des Übereinkommens Nr. 108 zu vollenden, als auch das Europäische Parlament und den Rat auf, den aktuellen Fortschritt in der Gesetzgebung zu erhalten.

Anlage 35

Europäische Datenschutzkonferenz vom 16. bis 17. Mai 2013 in Lissabon

Entschließung über die Zukunft des Datenschutzes in Europa

Der Datenschutz und der Schutz der Privatsphäre in Europa befinden sich momentan an einem wichtigen Wendepunkt, der markiert wird durch die Überarbeitung des Übereinkommens Nr. 108 des Europarates und der EU-Datenschutz-Richtlinie, zweier Hauptinstrumente, die die Eckpfeiler des Datenschutzes in ganz Europa darstellen.

Es ist daher an der Zeit, Bilanz zu ziehen und die Gelegenheit wahrzunehmen, zukünftige Herausforderungen zu bewältigen und den Weg zur Stärkung der Standards und der Effektivität des Datenschutzes in einer globalisierten Welt konsequent weiter zu beschreiten. Dies ist keine leichte Aufgabe und erfordert die engagierte Beteiligung aller Akteure in diesem dynamischen Prozess, mit besonderer Bedeutung für die Rolle der Datenschutzbehörden, die in erster Linie Behörden der Gewährleistung der Rechte des Einzelnen sind.

Die Modernisierung des Übereinkommens Nr. 108 und die EU-Datenschutzreform bieten Europa die Chance, auf den Erfahrungen für eine bessere Gestaltung der Zukunft aufzubauen, indem die in unserer Tradition verankerten hohen Werte und Prinzipien bestmöglich bei der Fortentwicklung des Schutzes der Privatsphäre in einer in technologischer und gesellschaftlicher Hinsicht grundlegend veränderten Welt gewahrt bleiben.

Die jetzt getroffenen Entscheidungen werden in den kommenden Jahren große Auswirkungen auf das Grundrecht der Bürger auf Datenschutz haben. Darüber hinaus gefährdet das Versäumnis, die Privatsphäre zu schützen, andere Rechte und Freiheiten, wie das Recht auf Nichtdiskriminierung, das Recht auf Freizügigkeit, das Recht auf Anonymität, das Recht auf freie Meinungsäußerung und letztlich die Menschenwürde. Zur Gewährleistung der wirksamen Ausübbarkeit der Grundrechte in einer demokratischen Gesellschaft ist es erforderlich, dass die notwendigen Garantien bestehen und jederzeit tatsächlich wahrgenommen werden können.

Im vollen Bewusstsein ihrer Aufgabe der Sicherung eines Grundrechts verpflichten sich die europäischen Datenschutzbeauftragten, weiterhin aktiv zur Entwicklung des Datenschutzes in allen Lebensbereichen in Europa beizutragen.

Die Frühjahrskonferenz der in Lissabon zusammen gekommenen europäischen Datenschutzbehörden

- fordert die europäischen Staaten, den Europarat und die Europäische Union auf, die Gelegenheit zur Überprüfung des Rechtsrahmens für den Datenschutz zu ergreifen, um die Rechte des Einzelnen zu stärken und einen wirksamen Schutz ihrer Privatsphäre in einer hoch technisierten und globalisierten Welt zu gewährleisten;

- bekräftigt die Notwendigkeit, einen einheitlichen und robusten Datenschutzrechtsrahmen zu entwickeln, der das gleiche Schutzniveau sowohl für den priva-

ten als auch den öffentlichen Sektor gewährt, unter Berücksichtigung der erforderlichen spezifischen Regelungen auf dem Gebiet der Strafverfolgung;

- äußert ihre tiefe Besorgnis darüber, dass unterschiedliche Strömungen bei der Reform des EU-Datenschutzes die Möglichkeit eröffnen, dass der Bereich der Strafverfolgung dem praktischen Schutzbereich des Grundrechts auf Datenschutz entzogen wird;

- fordert die EU-Gesetzgeber auf, zur Vermeidung einer gefährlichen rechtlichen Lücke im Datenschutz die Datenschutzverordnung und die Richtlinie gleichzeitig zu verabschieden, insbesondere in Anbetracht der zunehmenden Weiterverwendung von privaten Stellen verarbeiteter personenbezogener Daten zu Strafverfolgungszwecken.

- appelliert an den Europarat und die Europäischen Union, den datenschutzrechtlichen Herausforderungen durch das Internet entschiedener durch Schaffung von Klarheit und Sicherheit für Unternehmen und betroffene Personen sowie die Entwicklung angemessener Schutzmechanismen für einen wirksamen Schutz der Rechte der Einzelnen und eine praktische Durchsetzung durch Datenschutzbehörden zu begegnen.

- ermutigt Unternehmen und Behörden und alle, die in Politik und Recht am Datenschutz beteiligt sind, sich um Datensicherheit als eine der wichtigsten Prioritäten der Datenverarbeitungstätigkeiten zu bemühen und darin zu investieren, damit die steigenden Risiken von Datenschutzverletzungen in der digitalen Welt bekämpft und die Privatsphäre der Bürger aktiv geschützt wird.

- betont die Notwendigkeit, angesichts der Entwicklung neuer Geschäftsmodelle die Kooperationsmechanismen zwischen den Datenschutzbehörden zu stärken und einen gemeinsamen Ansatz und Handlungsmöglichkeiten zu finden, um den Schutz der Rechte der Einzelnen in der Praxis zu gewährleisten, wobei die Unabhängigkeit der Datenschutzbehörden wechselseitig zu achten ist.

- unterstreicht die Notwendigkeit der angemessenen Verstärkung der regelmäßigen Zusammenarbeit und Unterstützung der Datenschutzbehörden auf EU-Ebene als Reaktion auf die erheblichen Anforderungen des enorm gewachsenen Austauschs personenbezogener Daten mittels zentraler oder dezentraler IT-Systeme sowie des grenzüberschreitenden Informationsaustauschs insbesondere durch die Strafverfolgungsbehörden, so dass die Datenschutzbehörden die Einhaltung des Datenschutzes besser kontrollieren können.

- bekräftigt die Wichtigkeit, die Datenschutzbehörden mit ausreichenden Befugnissen, Kompetenzen, finanziellen Mitteln und Ressourcen auszustatten, damit sie ihre Kontrolltätigkeiten in unabhängiger Art und Weise vollständig erfüllen können und damit sie in der Lage sind, den Schutz des Grundrechts der Bürger auf Datenschutz und Schutz der Privatsphäre zu gewährleisten.

- ermuntert alle Beteiligten, sich an der Diskussion zur Zukunft des Datenschutzes in Europa zu beteiligen und hierzu beizutragen.

Anlage 36

Europäische Datenschutzkonferenz vom 16. bis 17. Mai 2013 in Lissabon

Entschließung zur „Gewährleistung des Datenschutzes in einer transatlantischen Freihandelszone“

Sponsoren:

- Comissão Nacional de Protecção de Dados (CNPD), Portugal
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Deutschland

Unterstützt von:

- Commission Nationale de l'Informatique et des Libertés (CNIL), Frankreich
- Garante per la protezione dei dati personali (Garante), Italien
- Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO), Polen
- Agencia Espanola de Protección de Datos (AEPD), Spanien

Da ein vom US-Präsidenten angekündigtes Freihandelsabkommen mit den Vereinigten Staaten von der Europäischen Union begrüßt wird und es zahlreiche Hinweise darauf gibt, dass eine solche transatlantische Freihandelszone wirtschaftliche Vorteile für beide Volkswirtschaften bringt,

- erinnert die Konferenz daran, dass nach den Standards der Welthandelsorganisation (Allgemeines Abkommen über den Handel mit Dienstleistungen, Artikel XIV) Staaten berechtigt sind, die zur Gewährleistung des Schutzes personenbezogener Daten erforderlichen Maßnahmen zu verabschieden und durchzusetzen;

- begrüßt die Konferenz die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz;

- vertritt die Konferenz die Auffassung, dass, soweit sich die bevorstehenden Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über die transatlantische Freihandelszone auf Fragen des Datenschutzes auswirken könnten, das in der Europäischen Grundrechtecharta verankerte Grundrecht auf Datenschutz und die daraus abgeleiteten hohen Standards gefördert und eingehalten werden sollten;

- weist die Konferenz darauf hin, dass jede diesbezügliche Regelung sowohl „inhaltliche“ Grundsätze als auch Verfahrenserfordernisse wie zum Beispiel Regelungen zur Zweckbindung und Weitergabe von Daten, effektive Kontrolle durch eine unabhängige Behörde sowie Zugang zu behördlichen und gerichtlichen Rechtsbehelfen beinhalten muss. Die Frage nach den Möglichkeiten direkten Zugriffs auf Daten von privater Unternehmen durch Strafverfolgungs- und

Sicherheitsbehörden außerhalb der EU sollte ebenfalls angemessen thematisiert werden;

- betont die Konferenz, dass auch in einer transatlantischen Wirtschaftsunion die Anwendung der nach europäischem Recht garantierten Grundrechte sichergestellt werden muss. Die Verhandlungen sollen sich nicht auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken;

- erwartet die Konferenz, dass die inspirierende Idee eines transatlantischen umfassenden Handelsabkommens nicht nur das Wirtschaftswachstum erhöhen, sondern auch die Bemühungen für ein hohes Maß an Datenschutz in den USA und in der Europäischen Union voranbringen wird. Dabei darf man nicht vergessen, dass Datenschutz weltweit als ein erheblicher Wettbewerbsvorteil anerkannt wird.

Anlage 37

Europäische Datenschutzkonferenz vom 16. bis 17. Mai 2013 in Lissabon

Entschließung zur Sicherstellung eines angemessenen Datenschutzniveaus bei Europol

Sponsoren:

- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Deutschland
- College Bescherming Persoonsgegevens (CBP), Niederlande,
- Garante per la protezione dei dati personali (Garante), Italien
- Comissão Nacional de Protecção de Dados (CNPD), Portugal

Am 27. März 2013 hat die Europäische Kommission einen Vorschlag für eine Verordnung gemäß Artikel 88 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) vorgestellt. Dieser Verordnungsentwurf ändert inhaltlich grundlegend und weitreichend die geltende Rechtsgrundlage für das Europäische Polizeiamt (Europol) – den Beschluss des Rates vom 6. April 2009 zur Errichtung Europols (2009/371/JI - ABl. L 121/37). Hierzu erklärt die Konferenz:

Mit der neuen Rechtsgrundlage soll Europol neue Aufgaben wahrnehmen und zusätzliche Befugnisse erhalten. Nach dem Willen der Kommission soll die Datenverarbeitung Europols nicht länger gemäß den im geltenden Recht definierten Systemen und Dateien erfolgen, um die Möglichkeiten Europols für eine Verknüpfung der Daten aus bzw. mit unterschiedlichen Systemen nicht zu behindern. Mit dem Verordnungsentwurf soll die Analysetätigkeit Europols in größtmöglicher Weise flexibilisiert werden, da die Analyse nach Ansicht der Kommission der „Grundpfeiler“[5] der modernen, „informationsauswertenden“[6] Strafverfolgungstätigkeit ist.

Angesichts der erweiterten Möglichkeiten zur Verarbeitung personenbezogener Daten muss für Europol der Datenschutz auf hohem Niveau gewährleistet werden. Dies ergibt sich auch aus Art. 8 der Europäischen Grundrechtecharta, der hohe Anforderungen an den Schutz der Privatsphäre und personenbezogener Daten stellt. Einrichtungen der EU, die – wie Europol – in großem Umfang personenbezogene Daten verarbeiten, sind diesen Vorgaben in besonderer Weise verpflichtet.

Keinesfalls wäre es hinzunehmen, wenn die neue Rechtsgrundlage das bestehende Datenschutzniveau absenken würde. Genau dies ist aber zu befürchten – legt man den von der Kommission vorgelegten Entwurf zu Grunde. Mit dem Wegfall der bestehenden Europol-Systeme und -Dateien würden systemspezifische Sicherungen

---

[5] „Cornerstone“ (öffentliches Memo der Europäischen Kommission vom 27. März 2013, (Memo/13/286) „Questions and Answers: Enhancing Europol´s support to law enforcement cooperation and training“, S. 1).

[6] „intelligence-led” (a.a.O.)

entfallen, wie z. B. die im Europol-Beschluss und den Begleitregelungen enthaltenen engen Zweckbegrenzungen und Vorgaben für die Verarbeitung personenbezogener Daten in Analysedateien. Es scheint, als sollten durch den Kommissionsvorschlag bestehende Verfahrenssicherungen eingeschränkt sowie geltende Beschränkungen für die Datenübermittlung an Drittstaaten und -stellen aufgehoben werden.

Die Konferenz der europäischen Datenschutzbeauftragten fordert das Europäische Parlament, den Rat, und die Kommission auf, dafür zu sorgen, dass die neue Rechtsgrundlage für Europol den folgenden Anforderungen entspricht und dass die Kommissionsvorschläge in diesem Sinne nachgebessert werden.

1. Daten unschuldiger Personen (Opfer, Zeugen, Kontaktpersonen etc.) dürfen nur unter sehr strengen Voraussetzungen verarbeitet werden und bedürfen dabei besonderen Schutzes.

2. Betroffenenrechte.

3. Verfahrensgarantien.

4. Unabhängige und effiziente Datenschutzkontrolle, sowohl extern als auch innerhalb von Europol, zur Gewährleistung eines effizienten Datenschutzes unter aktiver Beteiligung der nationalen Datenschutzbehörden.

5. Ein angemessenes Datenschutzniveau bei der Kooperation mit Drittstaaten und mit sonstigen Stellen außerhalb der EU.

6. Eine strenge Zweckbindung für die Verarbeitung personenbezogener Daten.

Internationale Datenschutzkonferenz

Anlage 38

33. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre vom 1. bis 3. November 2011 in Mexiko

Entschließung „Die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)“

Sponsor:

- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Unterstützt von:

- Privacy Commission, Belgien
- Privacy Commissioner of Canada
- Information and Privacy Commissioner of Ontario/Canada
- Information Commissioner, Vereinigtes Königreich
- Institute for Access to Information, United Mexican States

Heute hat sich das Internet zur wichtigsten Technologie für die Übermittlung jeder Art von Kommunikation entwickelt, sei es Sprache, Video oder Daten, und es wurde zur Grundlage fast aller geschäftlicher Transaktionen und sozialer Interaktionen. Angesichts der drohenden Erschöpfung der Adressen, die vom gegenwärtig genutzten Internet Protokoll Version 4 (IPv4) zur Verfügung gestellt werden, angesichts der anhaltenden enormen weltweiten Nachfrage für Internetadressen und angesichts der Notwendigkeit des Internets zur Unterstützung einer wachsenden Palette neuer Geräte, einschließlich Sensoren und intelligenter Zähler (das „Internet der Dinge“), wurde ein neues Internetprotokoll (IPv6 – IP Version 6) standardisiert, entwickelt und im Laufe der letzten 10 Jahren getestet und muss nun umgesetzt werden.

Obwohl IPv6 im Vergleich zu IPv4 eine Reihe praktischer Vorteile aufweist, können seine Eigenschaften auch zu bestimmten Risiken für den Datenschutz und die Privatsphäre führen, was von der Konfiguration des neuen Protokolls und vor allem von der für die Zuteilung und Zuweisung der IPv6-Adresse gewählten Strategie abhängt. Diese Risiken müssen beim Einsatz der neuen Version des Internetprotokolls angesprochen und kontrolliert werden.

Die Internationale Konferenz gibt folgende Empfehlungen:

- Die Nutzung temporärer und nicht permanenter IPv6-Adressen („dynamische Adressen“) muss für jeden Nutzer durch die Beibehaltung der dynamischen Zuweisung von IPv6-Adressen durch ISPs möglich bleiben. Internetzugangsanbieter und Betreiber von Gateways sollte die Nutzung dynamischer IP-Adressen als

Standardeinstellung anbieten. Nutzer sollten außerdem in der Lage sein, ihre IP-Adresse während einer Sitzung durch einfaches Verfahren zu ändern. Die Gesetzgeber oder Regulierungsbehörden sollten, soweit erforderlich, es in Erwägung ziehen, entsprechende Verpflichtungen in ihre nationalen Rechtsrahmen hinzuzufügen, sofern dies nicht bereits geschehen ist.

- Der Einsatz temporärer und nicht permanenter IPv6-Adressen muss mit den IPv6-Autokonfigurationsfunktionen möglich bleiben, indem alle vorhandenen Möglichkeiten der Pseudorandomisierung der Schnittstellenkennung („Privacy Extensions“) genutzt werden. Gerätehersteller – vor allem Hersteller mobiler Geräte – sollten solche Möglichkeiten schnell in ihre Produkte integrieren. Der Einsatz dynamischer Adressen für Endgeräte sollte als Standardfunktion aktiviert werden.

- Als Standardeinstellung sollten Anbieter, Protokolle, Produkte und Dienstleistungen die Nutzung temporärer und nicht permanenter Adressen anbieten.

- Wie jeweils anwendbar, sollten Netzwerke und Applikationen alle Sicherheitsfunktionen von IPv6 (IPSec) in vollem Umfang nutzen, um die Sicherheit, Integrität und Vertraulichkeit zu gewährleisten.

- Immer wenn Standortinformationen für die Nutzung der Dienste auf mobilen Geräten und anderen über IPv6 verbundenen Geräten notwendig sind, sollten solche Informationen z. B. durch Verschlüsselung gegen rechtswidriges Abhören und Missbrauch geschützt werden.

- Alle für die Ausarbeitung und Umsetzung aller weiteren Entwicklungen des IP-Protokolls verantwortlichen Akteure müssen sicherstellen, dass solche Normen und Vorgaben die Datenschutzrechte und Werte von Anfang an vollständig berücksichtigen.

Die Internationale Konferenz begrüßt es, dass die International Working Group on Data Protection in Telecommunications (IWGDPT) derzeit über einen umfassenden Bericht zu diesen Fragen diskutiert. In dem Bericht sollen insbesondere die Auswirkungen einer datenschutzfreundlichen Umsetzung von IPv6 auf dem Gebiet der Strafverfolgung untersucht werden. Die IWGDPT wird gebeten, ihren Bericht unter Berücksichtigung der oben genannten Empfehlungen abzuschließen.

Anlage 39

34. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre vom 25. bis 26. Oktober 2012 in Punta del Este, Uruguay

Entschließung über die Zukunft des Datenschutzes

Unter Berücksichtigung der Diskussionen in der Europäischen Union über die Vorschläge für einen überarbeiteten Rechtsrahmen zum Datenschutz und der laufenden Arbeiten im Europarat und der OECD;

unter Berücksichtigung der in den USA laufenden Prozesse zur Verbesserung des Datenschutzes und insbesondere des Vorhaben, eine „Bill of Rights“ zum Datenschutz einzuführen;

unter Berücksichtigung der jüngsten, von der APEC ergriffenen Initiative die Zusammenarbeit zwischen Datenschutzbehörden zu stärken und ein System einfacher und überprüfbarer Datentransfers innerhalb der APEC und über ihre Grenzen hinaus durch die Regelungen grenzüberschreitender Datentransfers einzuführen;

unter Berücksichtigung des immer größer werdenden multilateralen Netzwerks und seiner Initiativen zur Förderung der Zusammenarbeit der internationalen Datenschutzbehörden bei der Durchsetzung des Datenschutzes;

unter Begrüßung der Tatsache, dass viele Länder in den letzten Jahren neue Datenschutzbehörden geschaffen haben;

mit Bezug auf zunehmende Globalisierung und rasante technologischen Entwicklungen hat die 34. Internationale Datenschutzkonferenz beschlossen, dass Ihre Mitglieder folgende Schritte unternehmen sollen:

1. ihre Zusammenarbeit verstärken, um die mit den grenzüberschreitenden Datenübermittlungen verbunden Risiken koordiniert in Angriff zu nehmen, z. B. durch Zusammenarbeit in multilateralen Netzwerken zur Durchsetzung des Datenschutzes, und

2. Informationen und Fachwissen im größtmöglichen Umfang austauschen, um sicherzustellen, dass aus den knappen Ressourcen der Behörden maximaler Nutzen gezogen wird,

3. Möglichkeiten größerer Interoperabilität zwischen unterschiedlichen Rechtssystemen und Datenschutzregimen erkennen und nutzen.

Erläuterungen

Immer mehr Unternehmen sind in mehr als einem Land tätig und auch Regierungen kooperieren zunehmend miteinander, um gemeinsame Bedrohungen und Besorgnisse zu überwinden. Technologien wurden entwickelt, die die grenzüberschreitende Kommunikation und den Datenaustausch erleichtern. Dadurch werden täglich große Mengen personenbezogener Daten über Grenzen hinweg übermittelt.

Verschiedene dieser Technologien weisen auch selbst Risiken für den Datenschutz und die Privatsphäre auf. Vor allem das Internet stellt den Schutz der personenbezogenen Daten und der Privatsphäre der Menschen vor großen Herausforderungen, insbesondere in Verbindung mit der zunehmenden Nutzung mobiler Geräte.

Gesetzgeber auf der ganzen Welt sind deshalb überzeugt, dass die Vorschriften und Gesetze zum Datenschutz und zum Schutz der Privatsphäre überprüft werden müssen. Außerdem sind die Datenschutzbehörden angesichts der gestiegenen Anforderungen aufgefordert, enger zusammenzuarbeiten und zu versuchen, ihre Handlungen soweit wie möglich zu koordinieren. Wegen der derzeitigen schwierigen wirtschaftlichen Lage weltweit ist es von entscheidender Bedeutung, Informationen und Fachwissen auszutauschen und den besten Nutzen aus knappen Ressourcen zu ziehen.

Derzeit werden in allen Teilen der Welt die datenschutzrechtlichen Regelungen überprüft. Es wird die große Chance geboten, zu versuchen, die verschiedenen Systeme miteinander in Einklang zu bringen. Wir müssen diese Chance ergreifen, um allen Menschen auf der ganzen Welt einen besseren Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten zu bieten.

Anlage 40

34. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre vom 25. bis 26. Oktober 2012 in Punta del Este, Uruguay

Entschließung zu Cloud Computing

Cloud Computing (CC) gewinnt zunehmend an Interesse, weil es eine größere Wirtschaftlichkeit, weniger Belastung für die Umwelt, einfachere Handhabung, mehr Benutzerfreundlichkeit und viele andere Vorteile verspricht. Aufgrund folgender Tatsachen wirft die Entwicklung von CC viele wichtige Themen auf, wie z. B. in folgender Hinsicht: Die Technologie befindet sich noch im Entwicklungsstadium, die Datenverarbeitung findet jetzt weltweit statt, und aufgrund der fehlenden Transparenz wird die Durchsetzung von Regelungen zum Schutz der Privatsphäre und der Daten sogar noch erschwert. Dadurch könnten die Risiken, die bei der Datenverarbeitung auftreten, noch erhöht werden, wie Verstöße gegen die Datensicherheit, Verstöße gegen Gesetze und Grundsätze für den Schutz der Privatsphäre und der Daten, und der Missbrauch der in der Cloud gespeicherten Daten.

Die Mitglieder der Internationalen Konferenz und andere Interessengruppen, wie zum Beispiel die International Working Group on Data Protection in Telecommunications (IWGDPT, auch bekannt als „Berlin Group“[7]), hat die mit CC verbundenen datenschutzrechtlichen Probleme untersucht.

Ohne dabei eine von einer bestimmten Gruppe vorgenommene Analyse zu unterstützen, begrüßt die Internationale Konferenz derartige Bemühungen. Um einen Beitrag für die Förderung solcher Bemühungen und zur Vermeidung der mit der Nutzung der Cloud Computing Dienste verbundenen Risiken und zur Förderung der Verantwortlichkeit und der ordnungsgemäßen Geschäftsführung zu leisten, empfiehlt die Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre deshalb:

- Im Vergleich mit anderen Arten der Datenverarbeitung darf Cloud Computing nicht zur Absenkung der Datenschutzstandards führen;

- die verantwortlichen Stellen sollen vor der Aufnahme von CC-Projekten die notwendigen Prüfungen der Auswirkungen und Risiken für den Datenschutz durchführen (ggf. durch vertrauenswürdige Dritte)

- Die Anbieter von Cloud-Diensten sollen angemessene Transparenz, Sicherheit, Verantwortlichkeit und Vertrauen in CC-Lösungen gewährleisten, insbesondere in Bezug auf Informationen über die Verletzung des Schutzes personenbezogener Daten und in Bezug auf Vertragsklauseln, die gegebenenfalls die Datenportabilität und Datenkontrolle durch Cloud-Nutzer unterstützen. Wenn sie als verantwortliche Stellen handeln, sollen Cloud-Diensteanbieter den Nutzern gegebenenfalls wichtige Informationen über mögliche Auswirkungen auf den

[7] Siehe z. B. das Arbeitspapier der Gruppe „Cloud Computing – Privacy and data protection issues (Sopot Memorandum)“, Sopot (Polen), 23. und 24. April 2012; http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

Datenschutz und über mit deren Dienste verbundene Risiken zur Verfügung stellen.

- Es sollen weitere Bemühungen im Bereich der Forschung, der Zertifizierung durch Dritte, Standardisierung, „Privacy by Design“- Technologien und anderen, damit verbundenen Systemen unternommen werden, um das gewünschte Maß an Vertrauen in CC zu erreichen. Um den Datenschutz gründlich und wirksam in Cloud Computing einzubauen, sollten schon im Anfangsstadium angemessene Maßnahmen in die Architektur von IT-Systemen und Geschäftsabläufen einbezogen werden (Privacy by Design).

- Die Gesetzgeber sollen die Angemessenheit und Interoperabilität der bestehenden Rechtsrahmen zur Erleichterung grenzüberschreitender Datenübermittlungen überprüfen, und sie sollten zusätzliche notwendige Maßnahmen zum Datenschutz im Bereich CC in Erwägung ziehen.

- Die Datenschutzbehörden sollen den verantwortlichen Stellen, Anbietern von Cloud-Diensten und Gesetzgebern weiterhin mit Informationen zu Fragen hinsichtlich des Schutzes der Privatsphäre und personenbezogener Daten zur Verfügung stehen.

Alle Interessengruppen – Anbieter, Kunden von CC und auch Regulierungsbehörden – sollten zusammenarbeiten, um ein hohes Datenschutzniveau und eine hohe IT-Sicherheit zu gewährleisten.

Anlage 41

35. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 23. bis 26. September 2013 in Warschau, Polen

Entschließung über digitale Bildung für alle

Eingedenk der wichtigsten geltenden internationalen Übereinkommen, von denen sich einige auf die grundlegenden Menschenrechte, den Datenschutz und den Schutz der Privatsphäre beziehen:

- Die Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948 – Artikel 25 und 26-3;
- Die Europäische Konvention zum Schutze der Menschen und Grundfreiheiten vom 4. November 1950 – Artikel 8;
- Die Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 – Artikel 241;
- Der Internationale Pakt der Vereinten Nationen über wirtschaftliche, soziale und kulturelle Rechte vom 16. Dezember 1966 – Artikel 17;
- Die Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Europarat, 28. Januar 1981 und das Zusatzprotokoll zur Konvention 108;
- Die OECD-Richtlinien über den Datenschutz;
- Das Memorandum von Montevideo über den digitalen Ausschluss von Jugendlichen;

Eingedenk der internationalen Übereinkommen, die sich unmittelbar auf die Rechte von Kindern beziehen:

- Die Genfer Erklärung der Kinderrechte vom 26. September 1924;
- Die UN-Kinderrechtskonvention vom 20. November 1989;
- Das Europäische Übereinkommen über die Ausübung von Kinderrechten, Europarat, Nr. 160, vom 25. Januar 1996.

Eingedenk der folgenden, auf der 30. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre im Jahr 2008 angenommenen Entschließungen:

- Die Entschließung zum „Datenschutz in sozialen Netzwerkdiensten“;
- Die Entschließung zum „Schutz der Privatsphäre von Kindern im Internet“, die die Beauftragten zur Entwicklung der digitalen Erziehung, insbesondere für die Jüngsten, ermutigt.

Gestützt auf die Entschließung zu „Privacy by Design“, die auf der 32. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre im Jahre 2010 angenommen wurde;

Gestützt auf die „Empfehlung des Rates zum Schutz der Kinder im Internet“ der OECD vom 16. Februar 2012,

Eingedenk der Empfehlung R(2006)12 des Europarates an die Mitgliedstaaten, angenommen am 27. September 2006 durch das Ministerkomitee, zur Befähigung von Kindern zum Umgang mit den neuen Informations- und Kommunikationstechnologien, und der “Erklärung des Ministerkomitees zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet“, angenommen am 20. Februar 2008;

Gestützt auf den Internationale Pakt der Vereinten Nationen über wirtschaftliche, soziale und kulturelle Rechte vom 16. Dezember 1966, – Artikel 13, der das Recht eines jeden auf Bildung anerkennt;

Eingedenk, dass die digitale Technologie heute zu einem Teil des täglichen Lebens geworden ist und vollständig in jeden Bereich unserer Existenz integriert ist: Soziale Beziehungen, Familie, Freunde, berufliche Tätigkeit, Konsum, kulturelle Aktivitäten, Freizeitaktivitäten; dass all diese Facetten nun mit dem digitalen Universum verwoben sind; dass dieses neue digitale Zeitalter die ganze Bevölkerung betrifft, unabhängig von Alter, Erfahrung und Standort.

In der Erkenntnis der Herausforderung, die Komplexität der digitalen Umgebung zu verstehen, da sich die Informationstechnologie rasch ändert, die an diesem Ökosystem beteiligten Akteure und das auf sie gegründete Geschäftsmodell. Deshalb sind die Nutzer und die politischen Entscheidungsträger nicht in der Lage, alle Risiken und alle Möglichkeiten für Innovation und Wirtschaftswachstum zu verstehen, die diese digitale Technologie bietet.

In der Einsicht, dass die digitale Technologie viele neue Herausforderungen in Bezug auf den Schutz der Daten und der Privatsphäre hervorruft und dass der rechtliche Rahmen allein nicht alle erforderlichen Antworten und Garantien zu geben vermag.

Die auf der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vertretenen Behörden erachten folgendes als dringend notwendig:

- **Die unverzügliche Förderung** des Wissens über die digitale Technologie, um es jedem Bürger, Konsumenten und Unternehmer zu ermöglichen, aktive, kreative und kritische Akteure zu werden, die über hinreichende Kenntnisse und ein ausreichendes Verständnis verfügen, um eine informierte Entscheidung über die Nutzung der von der digitalen Technologie angebotenen Möglichkeiten zu treffen;

- **Zusammenzuarbeiten**, in Verbindung mit allen wichtigen Beteiligten, da es hier um eine gemeinsame Verantwortung geht.

Demzufolge ruft die Entschließung die Mitglieder-Behörden dazu auf, mit allen betroffenen Beteiligten zusammenarbeiten, um:

- Die digitale Kompetenz zu **fördern** und eine Rolle bei der Ausbildung aller betroffenen Teile der Öffentlichkeit zu spielen, jeden Alters, um ihnen folgendes zu ermöglichen:
    - Die zur Teilnahme an der digitalen Umgebung notwendigen Kenntnisse zu erwerben;
    - Informierte und verantwortliche Akteure in der digitalen Umgebung zu werden; und
    - Ihre Rechte wirksam zu nutzen und sich über ihre Pflichten bewusst zu sein.
- Ein gemeinsames Programm über die digitale Ausbildung anzunehmen, das auf 5 Grundprinzipien und auf 4 operationellen Zielen beruht.

Grundprinzipien:

1. Minderjährige sind im Hinblick auf die digitale Technologie besonders zu schützen;
2. Lebenslanges Training zum Thema digitale Technologie ist zu fördern;
3. Zwischen den Möglichkeiten und Risiken der digitalen Technologien ist ein angemessener Ausgleich zu suchen;
4. Die Entwicklung guter Bräuche und der Respekt für andere Nutzer sind zu fördern;
5. Kritisches Denken zu Risiken und Vorteilen der digitalen Technologie ist zu fördern.

Operationelle Ziele:

1. Förderung der Ausbildung zum Thema Datenschutz als Teil des Programms zum Erwerb digitaler Kompetenz;
2. Eine Rolle beim Training von Kontaktpersonen zu spielen durch die Organisation des „Trainings der Trainer“ zum Schutz der Daten und der Privatsphäre oder hierzu beitragend;
3. Förderung von Berufen im Bereich der digitalen Technologien durch Förderung innovativer Sektoren, vor allem von Sektoren, die „Privacy by Design“ entwickeln;
4. Formulierung von Empfehlungen und guten Praktiken zur Nutzung der neuen Technologien für die betroffene Öffentlichkeit (Kinder, Eltern, Lehrer, Unternehmen ...).

Eine Arbeitsgruppe zur Umsetzung dieser operationellen Ziele wird eingerichtet.

Erläuternde Anmerkungen

In den letzten Jahren haben viele Datenschutzbehörden, die die wichtigsten regionalen Gebiete der Welt repräsentieren, ihre Erfahrungen ausgetauscht und wichtige Initiativen für das globale Bewusstsein von Kindern, Jugendlichen und im Bildungsbereich für den Datenschutz und die Privatsphäre ergriffen.

Diese Entschließung ist eine Fortsetzung der auf der 30. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre angenommenen Entschließung und zielt darauf ab, noch einen Schritt weiter zu gehen. Diese konkreten Vorschläge zielen auf die Förderung von Wissen über die digitale Technik und die Ausbildung aller betroffenen Teile der Öffentlichkeit, jeden Alters, ab. Dies soll allen Bürgern die Möglichkeit geben, sich zu informieren und verantwortungsvolle Akteure im digitalen Umfeld zu werden, ihre Rechte und Pflichten wirksam zu nutzen und sich über ihre Pflichten in diesem Universum bewusst zu werden. Daher ist eine groß angelegte Aktion erforderlich, die auf alle Teile der Öffentlichkeit abzielt.

Die Datenschutzbehörden könnten sich an ihre jeweiligen Regierungen wenden, um in weitem Umfang Maßnahmen (gesetzgeberischer Art oder in Zusammenarbeit mit allen wichtigen Akteuren, einschließlich der Zivilgesellschaft) auch auf internationaler Ebene zu ergreifen.

Die Datenschutzbehörden verpflichten sich zu langfristigem Handeln und regelmäßiger Bewertung der ergriffenen Maßnahmen, um eine effektive Fortsetzung der Empfehlungen dieser Entschließung sicherzustellen

Anlage 42

35. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 23. bis 26. September 2013 in Warschau, Polen

Entschließung zur Profilbildung

Nach der Erörterung der Frage zur Profilbildung während der geschlossenen Sitzung auf ihrer 34. Internationalen Konferenz in Uruguay und nach Anhörung verschiedener Experten aus dem öffentlichen und dem privaten Bereich während dieser geschlossenen Sitzung;

In Anerkennung der vielen nützlichen Anwendungen von großen Datenmengen und der Vorteile, die umfangreiche Datensammlungen für unterschiedliche Teile der Gesellschaft, sowohl für Unternehmen und Regierungen als auch für gemeinnützige Organisationen, mit sich bringen könnten;

Unter gleichzeitiger Berücksichtigung, dass die Sammlung personenbezogener Informationen in großen Datenbanken und deren anschließende Nutzung Gefahren für den Schutz personenbezogener Daten und der Privatsphäre darstellen;

In Anbetracht der Tatsache, dass sich die Risiken noch erhöhen, wenn verschiedene Datensätze ohne angemessene Berücksichtigung des Schutzes dieser Daten und des Zwecks, für den sie ursprünglich gesammelt wurden, kombiniert werden;

Unter Hinweis auf die allgemeinen Grundsätze des Datenschutzes und der Privatsphäre;

Unter erneuter Bestätigung der im Jahr 2012 angenommenen Erklärung von Uruguay über die Profilbildung;

fordert die 35. Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre von allen die Profilbildung nutzenden Parteien:

1. Eine klare Bestimmung der Notwendigkeit und des praktischen Nutzens eines bestimmten Profilbildungsvorgangs und die Gewährleistung angemessener Schutzmaßnahmen vor dem Beginn der Profilbildung.

2. Die Begrenzung, im Einklang mit den Grundsätzen des Privacy-by-Design, der Vermutung und der Menge der gesammelten Daten auf das für den beabsichtigten rechtmäßigen Zweck erforderliche Maß, und die Gewährleistung, soweit angemessen, dass die Daten für den vorgesehenen Zweck hinreichend auf dem neuesten Stand und korrekt sind.

3. Die Gewährleistung, dass die Profile und die zugrunde liegenden Algorithmen einer ständigen Überprüfung unterliegen, um eine Verbesserung der Ergebnisse und die Verringerung falsch-positiver oder falsch-negativer Ergebnisse zu ermöglichen;

4. Die möglichst umfassende Unterrichtung der Gesellschaft über Profilbildungsvorgänge, einschließlich der Art und Weise, wie Profile zusammengeführt wer-

den und der Zwecke, für die Profile genutzt werden, womit sichergestellt werden soll, dass die Einzelnen in der Lage sind, so weit wie möglich und soweit es angemessen ist, die Kontrolle über ihre eigenen personenbezogenen Daten zu behalten.

5. Die Gewährleistung, insbesondere in Bezug auf Entscheidungen, die bedeutende rechtliche Auswirkungen für die Einzelnen haben oder ihre Unterstützung oder ihren Status betreffen, dass die Einzelnen über ihr Recht auf Auskunft und Berichtigung unterrichtet werden und dass, soweit angemessen, menschliche Eingriffe vorgesehen sind, zumal angesichts der Zunahme der Vorhersagekraft von Profilen aufgrund effizienterer Algorithmen.

6. Die Sicherstellung, dass alle Profilbildungsvorgänge einer angemessenen Aufsicht unterliegen.

Außerdem rufen die Datenschutzbeauftragten die Regierungen der ganzen Welt dazu auf, die Offenheit zu gewährleisten und den Beteiligten Gelegenheit zu öffentlichen Stellungnahmen und Beiträgen bei allen Gesetzgebungsverfahren zu geben, die Profilbildungsvorgänge ins Werk setzen könnten.

Anlage 43

35. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 23. bis 26. September 2013 in Warschau, Polen

Entschließung zu Web Tracking und Datenschutz

Web Tracking ermöglicht den Organisationen die Überwachung fast jedes einzelnen Aspekts des Nutzerverhaltens im Internet. Die Art von Information, die durch Tracking erhoben werden kann, (z. B. IP-Adressen, Gerätekennungen, etc.), kann zur Identifizierung eines bestimmten Betroffenen führen. Diese Fähigkeit eröffnet den Organisationen die Möglichkeit zur Entwicklung eines umfangreichen Profils über die Online-Aktivitäten eines identifizierbaren Betroffenen über einen längeren Zeitraum.

Daten über Nutzeraktivitäten, die von einem Computer oder einem anderen Gerät (z. B. einem Smartphone) während der Nutzung verschiedener Dienste der Informationsgesellschaft im Internet erhoben werden, werden zunehmend von unterschiedlichen Akteuren für verschiedene Zwecke kombiniert, korreliert und analysiert, die sich von karitativen bis zu kommerziellen Zwecken der unterschiedlichen Akteure erstrecken, die solche Dienstleistungen oder Teile davon anbieten. Die erzeugten Interessenprofile (oder „Nutzerprofile“) können mit Daten der „offline-Welt“ über fast jeden Aspekt des Privatlebens, einschließlich finanzieller Informationen wie auch Informationen, beispielsweise über Freizeitinteressen, gesundheitliche Probleme, politische Ansichten und/oder religiöse Meinungen angereichert werden.

Wir erkennen an, dass Tracking den Verbrauchern einige Vorteile wie Netzwerk-Management, Sicherheit und Betrugsprävention bietet und die Entwicklung neuer Produkte und Dienstleistungen erleichtern kann. Dennoch stellt Tracking ein ernsthaftes Risiko für die Privatsphäre der Bürger in einer Informationsgesellschaft dar, denn es droht, die wichtigsten datenschutzrechtlichen Grundsätze der Transparenz, Zweckbindung und individuellen Kontrolle zu untergraben.

Als Konsequenz hieraus sollten alle Beteiligten, einschließlich Regierungen, internationale Organisationen und Anbieter von Informationsdiensten den Schutz der Privatsphäre beim Design, der Bereitstellung und Nutzung von Diensten der Informationsgesellschaft an die erste Stelle setzen.

Die Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre fordert daher alle Beteiligten auf, soweit es relevant und angebracht ist, Folgendes zu unternehmen:

- Beachtung des Grundsatzes der Zweckbindung;
- Benachrichtigung und Kontrolle über die Verwendung von Tracking-Elementen, einschließlich Geräte- und Browser-Fingerprinting;
- Verzicht auf die Nutzung unsichtbarer Tracking-Elemente zu anderen Zwecken als für Sicherheit bzw. Betrugsaufdeckung oder Netzwerk-Management;
- Verzicht auf die Ableitung eines Satzes an Informationselementen (Fingerabdrücke) für die alleinige Identifizierung und Verfolgung von Nutzern zu ande-

ren Zwecken als für Sicherheit bzw. Betrugsprävention oder Netzwerk-Management;

- Gewährleistung angemessener Transparenz über alle Arten von Web-Tracking-Verfahren, damit die Verbraucher eine informierte Wahl treffen können;

- Angebot einfach zu bedienender Werkzeuge, um den Nutzern angemessene Kontrolle über die Erhebung und Nutzung ihrer personenbezogenen Daten zu ermöglichen;

- Vermeidung des Trackings von Kindern und des Trackings auf an Kinder gerichteten Webseiten;

- Beachtung des Grundsatzes des Privacy-by-Design und Durchführung einer Datenschutz-Folgenabschätzung zu Beginn neuer Projekte;

- Verwendung von Techniken, die die Auswirkungen auf die Privatsphäre mindern, wie Anonymisierung bzw. Pseudonymisierung;

- Förderung technischer Standards für eine bessere Nutzerkontrolle (z. B. ein wirksamer Do-Not-Track-Standard).

Die Datenschutzbeauftragte der Republik Slowenien und die Französische Datenschutzbehörde enthielten sich bei der Abstimmung über diese Entschließung.

Anlage 44

35. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 23. bis 26. September 2013 in Warschau, Polen

Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht

Die Konferenz ruft in Erinnerung, dass sie:

- bereits auf ihrer 27. Sitzung in Montreux die Vereinten Nationen aufgefordert hat, ein verbindliches Rechtsinstrument vorzubereiten, in dem die Rechte auf Datenschutz und dem Schutz der Privatsphäre als einklagbare Menschenrechte klar und detailliert geregelt sind,

- auf ihrer 28. Sitzung in Montreal die Verbesserung der internationalen Zusammenarbeit beim Datenschutz und dem Schutz der Privatsphäre gefordert hat,

- auf ihrer 30. Sitzung in Straßburg eine Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz der personenbezogenen Daten verabschiedet hat,

- auf ihrer 31. Sitzung in Madrid internationale Standards zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre angenommen hat (Erklärung von Madrid),

- auf ihrer 32. Sitzung in Jerusalem die Regierungen zur Einberufung einer Regierungskonferenz aufgefordert hat, um ein verbindliches internationales Übereinkommen zum Schutz der Privatsphäre und der Daten zu erarbeiten, mit dem die Erklärung von Madrid umgesetzt wird,

und sie erinnert an die Wichtigkeit bestehender Instrumente im internationalen Recht, die Regelungen und Standards für den Schutz personenbezogener Daten vorsehen, insbesondere das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108).

Die 35. Internationale Konferenz stellt fest,

dass eine dringende Notwendigkeit für eine verbindliche internationale Vereinbarung zum Datenschutz besteht, die die Menschenrechte durch den Schutz der Privatsphäre, der personenbezogenen Daten und der Integrität von Netzwerken gewährleistet und die Transparenz der Datenverarbeitung erhöht, und dabei ein ausgewogenes Verhältnis im Hinblick auf Sicherheit, wirtschaftliche Interessen und freie Meinungsäußerung wahrt.

und beschließt

die Regierungen aufzufordern, sich für die Verabschiedung eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) einzusetzen, das auf den Standards, die von der Internationalen Konferenz entwickelt und gebilligt wurden, und auf den Bestimmungen im allgemeinen Kommentar Nr. 16 zum Pakt basieren sollte, um weltweit gültige Standards für den Datenschutz und den Schutz der Privatsphäre zu schaffen, die im Einklang mit der Rechtsstaatlichkeit stehen.

Sonstiges

Anlage 45

Organigramm

(Stand: 1. Oktober 2013)

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 der Aufsichtsbehörde nach § 38 BDSG *Virtualisierung der 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

A

B

C

D

E

F

L

M

N

O

P

Q

R

S

T

U

V

W

Z