X. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz, 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

Nach den Datenskandalen der Jahre 2008 und 2009 im Verbraucher- und Arbeitnehmerbereich und Novellierungen des Bundesdatenschutzgesetzes setzte sich auch in den Folgejahren die Debatte über den grundlegenden Modernisierungsbedarf des Datenschutzrechts in Deutschland fort. Dazu trugen auch weitere Skandale im Jahre 2011 zumal bei IT-Konzernen mit bei. Infolge des Urteils des Bundesverfassungsgerichts zur Unzulässigkeit der Vorratsdatenspeicherung in der Telekommunikation blieb der Datenschutz auf der politischen Agenda. Mahnende Hinweise auf die Bedeutung der Privatsphäre im digitalen Zeitalter – nicht zuletzt auch etwa infolge des Starts des Dienstes Google Street View und allgemein angesichts der weit verbreiteten Nutzung sozialer Netze, jüngst auch in Verbindung mit Gesichtserkennungsdiensten – erfahren Zustimmung und zugleich Skepsis und Resignation. Die Volkszählung 2011 ist zwar kein Überwachungsfanal wie noch in den 80er Jahren des letzten Jahrhunderts, doch sind Datenschutz und Datensicherheit nicht minder vonnöten. In diesem Bericht werden die aktuellen Entwicklungen nachgezeichnet und kommentiert.

Auch in Sachsen-Anhalt gab es im Berichtszeitraum einige datenschutzrechtlich komplexe und langwierige Prüfvorgänge, die nicht nur datenschutzrechtliche Verstöße aufdeckten, sondern aus meiner Sicht mit zur Sensibilität in Bezug auf Datenschutzbelange beigetragen haben. Ohnehin ist der Datenschutz mehr und mehr auch zur Bildungsaufgabe geworden. In den Behörden fehlt es aber oft nicht nur am Datenschutzbewusstsein, sondern auch am unterstützenden Datenschutzmanagement.

Der Landtag von Sachsen-Anhalt wählte mich auf Vorschlag der Landesregierung im Dezember 2010 für eine zweite Amtsperiode, die Mitte März 2011 begann. Damit ist Kontinuität möglich. Prägend für die Zukunft und eine besondere Herausforderung wird die zusätzliche Wahrnehmung der Datenschutzaufsicht über den nicht-öffentlichen Bereich werden.

Der X. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2009 bis 31. März 2011. Bei einzelnen Beiträgen konnten noch aktuelle Sachstände einbezogen werden (Redaktionsschluss: 15. August 2011).

Allen, die mich bei meiner Tätigkeit unterstützt haben, danke ich vielmals. Mein besonderer Dank gilt wie bei den vergangenen Berichten wieder meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle für die geleistete Arbeit.

Magdeburg, den 1. September 2011

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

Inhaltsverzeichnis

Anlagenverzeichnis

Nationale Datenschutzkonferenz

Abkürzungsverzeichnis

A

AbgG LSA	Gesetz über die Rechtsverhältnisse der Mitglieder des Landtages von Sachsen-Anhalt (Abgeordnetengesetz Sachsen-Anhalt)
AG	Arbeitsgruppe
AG VIG LSA	Ausführungsgesetz zum Verbraucherinformationsgesetz Sachsen-Anhalt
AID	Identifikationsnummer des Auskunftspflichtigen
AKIF	Arbeitskreis Informationsfreiheit der Konferenz der Informationsfreiheitsbeauftragten
API	Application Programming Interface, Programmierschnittstelle für Anwendungen
ARGEn	Arbeitsgemeinschaften
ATA	Advanced Technology Attachment, Software-Protokoll im PC
AV	Ausführungsvorschrift
AZR	Ausländerzentralregister

B

BA	Bundesagentur für Arbeit
BAG	Bundesarbeitsgericht
BayStVollzG	Gesetz über den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Sicherungsverwahrung
BBhV	Verordnung über Beihilfe in Krankheits-, Pflege- und Geburtsfällen (Bundesbeihilfeverordnung)
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BIOS	Basic Input/Output System
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.
BKA	Bundeskriminalamt
BKADV	Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BKZ	Belegkennzeichen
BLFA- FE/FL	Bund-Länder Fachausschuss Fahrerlaubnis-/Fahrlehrerrecht
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz)
BtBG	Gesetz über die Wahrnehmung behördlicher Aufgaben bei der Betreuung Volljähriger (Betreuungsbehördengesetz)
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BWG	Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege
BZRG	Gesetz über das Zentralregister und das Erziehungsregister

C

CA	Certificate-Authority, Zertifizierungsstelle
CeBIT	Centrum für Büroautomation, Informationstechnologie und Telekommunikation
CIO	Chief Information Officer (deutsch: Leiter Informationstechnologie)
CSS	Cascading Style Sheets (Formatierungssprache im Internet)

D

D115	Projekt D115, einheitliche Behördenrufnummer für Deutschland
DCO	Device Configuration Overlay
DlStatG	Gesetz über Statistiken im Dienstleistungsbereich (Dienstleistungsstatistikgesetz)
DNS	Domain Name System
DNSSEC	DNS Security Extensions, Sicherheitserweiterung für das DNS
DOL	Aktionsplan Deutschland-Online
DOS	Disk Operating System
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
DVDV	Deutsche Verwaltungsdienste-Verzeichnis

E

EA	Einheitlicher Ansprechpartner
EAG LSA	Einheitlicher-Ansprechpartner-Gesetz des Landes Sachsen-Anhalt
EDSB	Europäischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
eID	elektronische Identifizierungsfunktion des nPA
EU-DSRL	Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG)
eGK	elektronische Gesundheitskarte
ELENA	Elektronischer Entgeltnachweis
ELStAM	elektronische Lohnsteuerabzugsmerkmale
E-Mail	Elektronischer Brief
EMRK	Konvention zum Gesetz der Menschenrechte und Grundfreiheiten
EnWG	Energiewirtschaftsgesetz
ePass	Elektronischer Reisepass
EU	Europäische Union
EU-DLR	EU-Dienstleistungsrichtline (Richtlinie 2006/123/EG)
EuGH	Europäischer Gerichtshof
E-ZensAG LSA	Entwurf eines Ausführungsgesetzes des Landes Sachsen-Anhalt zum Zensusgesetz 2011

F

FEB	Fahrerlaubnisbehörde
FeV	Fahrerlaubnisverordnung
FRZ	Finanzrechenzentrum

G

GDI	Geodateninfrastruktur
GDI-LSA	Geodateninfrastruktur des Landes Sachsen-Anhalt
GDIG LSA	Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt
GEREK	Gremium Europäischer Regulierungsstellen für elektronische Kommunikation
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
GGO LSA I	Gemeinsamen Geschäftsordnung der Ministerien – Allgemeiner Teil
GIAZ	Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus
GIW	Geoinformationswirtschaft
GO LSA	Gemeindeordnung für das Land Sachsen-Anhalt
GPS	Global Positioning System
GSM	Global System for Mobile Communications, Mobilfunkstandard, 2. Generation
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GÜL	Gemeinsame elektronische Überwachungsstelle der Länder
GVBl. LSA	Gesetz- und Verordnungsblatt für das Landes Sachsen-Anhalt

H

HÄV SH	Hausärzteverband Schleswig-Holstein e.V.
HPA	Host Protected Area
HSG	Hochschulgesetz des Landes Sachsen-Anhalt
HSTS	HTTP Strict Transport Security (Erzwungen verschlüsselter Transport)
HTML	Hypertext Markup Language (Hypertext-Auszeichnungssprache)
HTTP	Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll)
HTTPS	HyperText Transfer Protocol Secure (sicheres HTTP)
HwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung)
HZD	Hessische Zentrale für Datenverarbeitung

I

IaaS	Infrastructure as a Service
IAM	Identity and Access Management (Identitäts- und Zugriffsverwaltung)
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers

IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IHK	Industrie- und Handelskammer
IMI	Internal Market Information System (Binnenmarktinformationssystem)
iOS	Operating System (OS), Standard-Betriebssystem der Apple-Produkte iPhone, iPod touch, iPad
IP	Internet Protocol
IP-Adresse	Internetprotokoll-Adresse
Ipv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Informationstechnik (synonym: Informationstechnologie)
IT-KA	Koordinierungsausschuss 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 Land Sachsen-Anhalt
ITN XT	zukünftigen Landesnetzes – ITN-„eXTended“)
IT-PLR	IT-Planungsrat
IuK	Informations- und Kommunikationstechnik (synonym: Informations- und Kommunikationstechnologie)
IZG LSA	Informationszugangsgesetz Sachsen-Anhalt

J

JMStV	Jugendmedienschutz-Staatsvertrag
JSchrG LSA	Gesetz zur Aufbewahrung von Schriftgut der Justiz im Land Sachsen-Anhalt
JStVollzG LSA	Gesetz über den Vollzug der Jugendstrafe in Sachsen-Anhalt (Jugendstrafvollzugsgesetz)
JVA	Justizvollzugsanstalt

K

KBA	Kraftfahrt-Bundesamt
KOM	Europäische Kommission
KoopA ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich
KoSIT	Koordinierungsstelle für IT-Standards

L

LBG LSA	Beamtengesetz des Landes Sachsen-Anhalt
LDAP	Lightweight Directory Access Protocol
LHO	Landeshaushaltsordnung des Landes Sachsen-Anhalt
LIZ	Landesinformations-Zentrum in Halle (Saale); LHO Betrieb bis 31.12.2009
LL IS	Landesleitlinie Informationssicherheit
LReg.	Landesregierung
LRZ	Landesrechenzentrum (Abt. 4 der OFD Magdeburg)
LT-Drs.	Landtagsdrucksache

LTE	Long Term Evolution, Mobilfunkstandard, 4. Generation

M

MG LSA	Meldegesetz des Landes Sachsen-Anhalt
Mikrozensusgesetz 2005	Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte
MMS	Multimedia Messaging Service
MSI	Microsoft Installer, Dateiformat für Softwareinstallationsarchive
MSP	Microsoft Installer, Dateiformat für Aktualisierungen (Patches)

N

NADIS	Nachrichtendienstliches Informationssystem
NAT	Network Address Translation, Adressumsetzung in IT-Netzwerken
NEGS	Nationale E-Government Strategie
NfD	Nur für den Dienstgebrauch
NJW	Neue Juristische Wochenschrift
nPA	neuer Personalausweis
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA-RR	Neue Zeitschrift für Arbeits- und Sozialrecht – Rechtsprechungs-Report Arbeitsrecht

O

ÖbVermIngG LSA	Gesetz über die Öffentlich bestellten Vermessungsingenieure im Land Sachsen-Anhalt
ÖbVI	Öffentlich bestellter Vermessungsingenieur
OFD	Oberfinanzdirektion Magdeburg
OMP	Ordnungsmerkmal der Person
OSCI	Online Services Computer Interface
OSS	Open Source Software, Anwendungen mit offengelegtem Quelltext und freier Lizenz
OWiG	Gesetz über Ordnungswidrigkeiten

P

PaaS	Platform as a Service
PaßG	Paßgesetz
PC	Personalcomputer
PD	Polizeidirektion
PHP	PHP Hypertext Preprocessor, eine serverseitige Skriptsprach
PIN	Persönliche Identifikationsnummer
PlPr.	Plenar-Protokoll
PKI LSA	Public Key Infrastruktur Land Sachsen-Anhalt
PNR	Passenger Name Record
PON	Personenbezogene Ordnungsnummer

PPP	Public-Private-Partnership
PROMIS	Personal-, Ressourcen-, Organisationsmanagement- u. Informationssystem

Q

QES	Qualifizierte elektronische Signatur

R

RdErl.	Runderlass
RDV	Recht der Datenverarbeitung
RFID	Radio Frequency Identification (Radiofrequenz-Identifikation)
RIM	Research In Motion
RIPE NCC	Réseaux IP Européens Network Coordination Centre, ist eine RIR, zuständig u. a. für Europa
RIR	Regional Internet Registry; regional mit der Verwaltung und Zuteilung von Internet-Ressourcen betraute Organisation
RPKI	Routing Public Key Infrastructure
RRL	Rahmenrichtlinie

S

SALSA	Secure Access Land Sachsen-Anhalt
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SchwarzArbG	Gesetz zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung
Screening-ID	Screening-Identifikationsnummer
SGB	Sozialgesetzbuch
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil
SGB II	Zweites Buch Sozialgesetzbuch – Grundsicherung für Arbeitsuchende
SGB VII	Siebtes Buch Sozialgesetzbuch – Gesetzliche Unfallversicherung
SGB VIII	Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe
SGB IX	Neuntes Buch Sozialgesetzbuch – Rehabilitation und Teilhabe behinderter Menschen
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren
SMS	Short Message Service
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
Spam	Unverlangte E-Mail-Nachrichten, häufig Werbung oder Müll
SpielO-VO	Verordnung über die Spielordnung in öffentlichen Spielbanken
SSD	Solid State Drive
SSL	Secure Sockets Layer (Netzwerkprotokoll zur sicheren Datenübertragung)
StatG-LSA	Landesstatistikgesetz Sachsen-Anhalt
StGB	Strafgesetzbuch
StiftG LSA	Stiftungsgesetz Sachsen-Anhalt

StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung
SWIFT	Society for Worldwide Interbank Financial Telecommunication

T

TCloud	Trustworthy Cloud
TFTP	Terrorist Finance Tracking Program
ThUG	Gesetz zur Therapierung und Unterbringung psychisch gestörter Gewalttäter
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security (Netzwerkprotokoll zur sicheren Datenübertragung)
TMG	Telemediengesetz
TPM	Trusted Platform Module
TYPO3	Content-Management-Framework für Websites

U

UHS	User Help Desk (Benutzerbetreuung)
UMTS	Universal Mobile Telecommunications System, Mobilfunkstandard, 3. Generation
URL	Uniform Resource Locator, einheitlicher Quellenanzeiger
USB	Universal Serial Bus
UVollzG LSA	Gesetz über den Vollzug der Untersuchungshaft in Sachsen-Anhalt

V

VDV	Verband Deutscher Verkehrsunternehmen
VerfSchG LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermGeoG LSA	Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt
VG	Verwaltungsgericht
VoIP	Voice over IP, Telefonie über das Internet
VPN	Virtual Private Network (deutsch: virtuelles privates Netz)
VV-DSG-LSA	Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger
VV-LHO	Verwaltungsvorschrift zur LHO
VwVG	Verwaltungs-Vollstreckungsgesetz

W

WLAN	Wireless Local Area Network (drahtloses, lokales Netzwerk; lokales Funknetz)

X

XHTML	Extensible HyperText Markup Language (erweiterbare HTML, Standard)
XING	Soziales Netzwerk (x-ing, crossing)
XML	Extensible Markup Language (erweiterbare Auszeichnungssprache)
XÖV	fachliche Standards in der öffentlichen Verwaltung auf Basis von XML

Z

ZensAG LSA	Ausführungsgesetz des Landes Sachsen-Anhalt zum Zensusgesetz 2011
ZensG 2011	Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011)
ZFER	Zentrales Fahrerlaubnisregister
ZPO	Zivilprozessordnung
ZSS	Zentrale Speicherstelle
ZustVO GewAIR	Verordnung über die Regelung von Zuständigkeiten im Immissions-, Gewerbe- und Arbeitsschutzrecht sowie in anderen Rechtsgebieten
ZVG	Gesetz über die Zwangsversteigerung und die Zwangsverwaltung

1 Entwicklung und Situation des Datenschutzes

„Die anlasslose Speicherung von Telekommunikationsverkehrsdaten ist geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins und des ständigen Überwachtwerdens hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenhang mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Die Einführung einer Telekommunikationsverkehrsdatenspeicherung kann nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der schon vorhandenen Datensammlungen zu größerer Zurückhaltung. ***Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.*** *Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer."* (aus dem Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08 u. a.).

Die Freiheitsmaßstäbe des Bundesverfassungsgerichts, abgeleitet aus den Grundrechten des Grundgesetzes, bleiben Richtschnur für den Datenschutz, die datenschutzrechtlich verantwortlichen Stellen und die Datenschützer. Der Europäische Gerichtshof hat die unabhängigen Datenschutzbeauftragten als „Hüter von Grundrechten und Grundfreiheiten" bezeichnet (Urteil vom 9. März 2010, C-518/07, NJW 2010, 1265). Die Aufgabe ist unverändert anspruchsvoll und erfordert ein entsprechendes Verantwortungsbewusstsein. Der Landesbeauftragte bezieht in sein Verständnis der Aufgabenwahrnehmung auch die Leitaussage des Bundesverfassungsgerichts seit dem Volkszählungsurteil von 1983 ein, wonach Datenschutz bzw. informationelle Selbstbestimmung nicht nur subjektives Recht ist, sondern dass sich im objektiven Wertgehalt des Grundrechts auch eine Funktionsbedingung des demokratischen Gemeinwesens widerspiegelt (s. IX. Tätigkeitsbericht, Nr. 1).

Datenschutz ist Freiheitsmaßstab und Vertrauensfaktor. Das Vertrauen der Dateninhaber kann leiden, wenn der Staat beim Kampf gegen Kriminalität übermäßige Eingriffe in Persönlichkeitsrechte vornimmt und Betroffene sich infolgedessen in ihrer Verhaltensfreiheit auch bei anderen Grundrechtswahrnehmungen eingeschüchtert fühlen oder wenn der Staat der übermäßigen Datenverarbeitungspraxis der Wirtschaft nicht Einhalt gebietet und somit seine grundrechtliche Schutzaufgabe vernachlässigt. Nur wenn der Bürger und Konsument Vertrauen in das Datenschutzgebaren von Staat und Wirtschaft hat, wird er Angebote des E-Government oder E-Commerce in Anspruch nehmen.

Die eingangs zitierten Passagen aus dem Urteil des Bundesverfassungsgerichts zur Nichtigkeit der Vorratsspeicherung von Telekommunikationsver-

kehrsdaten beschreiben einen Kern der Freiheitsgrundrechte und zugleich den Nerv einer aktuellen Debatte, bei der es auch um das Verhältnis von europäischem und nationalem Recht geht (ausführlicher Nr. 25.1). Ohnehin wird der Datenschutz in Deutschland zunehmend durch europäische Entwicklungen geprägt werden; dabei handelt es sich nicht nur um die Ausweitung von Datensammlungen, sondern auch um ein der Grundrechtecharta der Europäischen Union entsprechendes Regelungswerk für den Datenschutz (vgl. Nr. 3.1).

Konzeptionen und Maßnahmen des Datenschutzes betreffen im Wesentlichen vier Bereiche: 1. Recht, 2. Technik, 3. Kontrolle und 4. Bildung oder Medienkompetenz (vgl. auch Grundsatzentschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009, **Anlage 1**; s. Nr. 1.4). In diesem Tätigkeitsbericht werden diese Bereiche übergreifend und anhand von Einzelvorhaben und Aktivitäten näher beschrieben.

Im Hintergrund steht dabei auch das merkwürdige Phänomen, dass private Daten einerseits für den Menschen, ob als Bürger oder als Verbraucher oder Internetnutzer, trotz eines insgesamt veränderten Verständnisses von Privatsphäre durchaus einen Wert haben im Sinne einer persönlichkeitsbezogenen Wertschätzung, ausgeprägt besonders etwa bei Konto- oder Gesundheitsdaten, und dass der Datenschutz im Verhältnis Bürger – Staat rechtspolitische Akzeptanz erfahren hat und weiter erfährt, andererseits aber Empfehlungen zu mehr Datensparsamkeit und Selbstdatenschutz insbesondere bei der Internetnutzung auf weniger Widerhall stoßen. Dies ist auch eine Anfrage an Konzepte und Methoden der Medienbildung (vgl. Nr. 21.2). Das Internet wird jedenfalls weit verbreitet als Privatsache empfunden, vermeintlich unbeobachtet und anonym wird die Technik, an die ohnehin eine Gewöhnung stattgefunden hat, gern genutzt. Doch das Internet vergisst nichts. Deshalb ist der Ansatz eines „Vergessens im Internet“ so wichtig, doch zugleich so schwierig (vgl. Nr. 1.3).

Der X. Tätigkeitsbericht des Landesbeauftragten umfasst den Zeitraum vom 1. April 2009 bis zum 31. März 2011. Darüber hinaus reichende Entwicklungen wurden soweit möglich mitberücksichtigt.

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),
- der Öffentlichkeitsarbeit (§ 22 Abs. 4a Satz 3 DSG-LSA),
- der Information der Behörden und behördlichen Datenschutzbeauftragten und interessierter Bürgerinnen und Bürger.

Der X. Bericht beinhaltet wiederum datenschutzpolitische Feststellungen und greift Grundsatzthemen auf. Er enthält Informationen, Kritik und Lob zu rechtlichen und technischen Entwicklungen. Dabei werden auch Kommentare der Landesregierung aus ihrer Stellungnahme zum IX. Tätigkeitsbericht (LT-Drs.

5/2385) einbezogen. Der aktuelle Bericht stellt Materialien und praxisbezogene Hinweise aus anschaulichen Einzelfällen, Beratungen und Kontrollen zur Verfügung.

Seit dem VII. Tätigkeitsbericht werden die Berichte nicht nur in den Ausschüssen des Landtages für Inneres und Recht und Verfassung, sondern auch im Plenum im Rahmen einer Debatte beraten und zur Kenntnis genommen. Diese gegenüber Vorgängerberichten abweichende Verfahrensweise geht auf einen Vorschlag des Landesbeauftragten zurück. Sie entspricht Wortlaut und Sinn der o. a. Gesetzesregelung und dem Gegenstand. Eine öffentliche Debatte zum Datenschutzbericht empfiehlt sich auf Dauer (vgl. auch Nr. 2.3).

1.1 Sicherheit und Freiheit

In vergangenen Tätigkeitsberichten ist die Entwicklung zum Präventionsstaat und die nicht tragende Rechtfertigung „Ich habe nichts zu verbergen." ebenso beschrieben wie der Abwehrcharakter der Grundrechte betont und vor dem Überwachungsstaat gewarnt worden. Der Rechtsstaat benötigt Selbstachtung, man stärkt ihn nicht dadurch, dass man seine Wurzeln beschädigt. Der Schutz durch den Staat, hergeleitet aus dem objektiven Gehalt der Grundrechte, hat den aus subjektiven Rechten hergeleiteten Schutz vor dem Staat zu wahren. In die nötigen Abwägungsprozesse im Verhältnis von Sicherheit und Freiheit gehört die Beachtung des Primats der Freiheit. Datenschutz ist nicht Hindernis, Datenschutz gehört zum Rechtsstaat; Datenschützer sind stets auch „Verfassungs-Schützer", sie unterstützen Demokratie und Rechtsstaat; wer dieses Grundrecht also stärkt und die es schützenden Institutionen, stärkt den Rechtsstaat (vgl. VIII. Tätigkeitsbericht, Nrn. 1.1, 1.4 und IX. Tätigkeitsbericht., Nrn. 1.1, 1.4). Diese grundsätzlichen Aussagen gelten unverändert.

Ohnehin fällt auf, dass es keineswegs immer die Wirtschaft oder auch der einzelne Internetnutzer ist, dessen Datenverarbeitung Sorgen bereitet. Staatliche Datensammlungen stehen nach wie vor mit im Fokus der Kritik. Sie sind hinsichtlich ihres Umfangs und ihrer Streubreite oftmals nicht mit den Freiheitsmaßstäben der Verfassung vereinbar. Ganz und gar nicht vorbildlich, ja widersprüchlich wirkt der Versuch des Staates, auf Datenskandale der Wirtschaft zu zeigen, auf eine zu freizügige Datenpreisgabe privater Nutzer zu verweisen und diese zugleich zu mehr Inanspruchnahme von E-Government und E-Commerce zu animieren, um dann aber bei der eigenen Datenverarbeitung Bürgerrechte zu missachten.

Aus dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08 – NJW 2010, 833) zur Vorratsdatenspeicherung ergibt sich auch (vgl. im Übrigen Nrn. 20.3, 25.1) das Gebot einer sog. **Überwachungs-Gesamtrechnung,** d. h. die Verpflichtung des Staates, den vorhandenen Stand staatlicher Überwachungssysteme und -maßnahmen im Falle der Erwägung neuer Speicherungspflichten – also vorher! – in eine Gesamtbetrachtung einzubeziehen und Maß zu halten (vgl. Roßnagel, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238). Dieser Gedanke findet sich bereits in der Entscheidung des Gerichts vom 12. April 2005 zur GPS-Überwachung und dem dort entwi-

ckelten Hinweis auf Gefahren durch additive Grundrechtseingriffe (BVerfGE 112, 304; vgl. VIII. Tätigkeitsbericht, Nr. 1.4).

Zusätzlich wird man aus dieser Überlegung heraus aber die Verpflichtung des Staates festhalten müssen, den vorhandenen Überwachungskatalog als solchen einer **Evaluation**, einer Überprüfung und damit auch einer Beschränkung auf die unbedingt erforderlichen Regelungen und Eingriffsmaßnahmen zu unterziehen (vgl. dazu auch die Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010, **Anlage 10**). „Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels muss der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung korrigierend eingreifen. Dies betrifft auch die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern." (BVerfG, a. a. O. in der GPS-Entscheidung). Dies ist eine schwierige Aufgabe, die dem Gesetzgeber damit zugemutet wird, und die besondere Anforderungen auch an die Politikberatung im digitalen Zeitalter stellt. Denn es geht dabei auch um die Umsetzung des Anspruchs aus dem neuen Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß dem Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/01 u. a., NJW 2008, 322; IX. Tätigkeitsbericht, Nr. 1).

Wer dann eine Verlängerung von Maßnahmen oder sogar zusätzliche, neue Befugnisse zumal für die Sicherheitsbehörden verlangt, muss nachvollziehbare Belege für die Eignung und Notwendigkeit bringen. Die Sicherheit wächst nicht dadurch, dass die Politik Instrumente plakativ nur fordert und dazu abstrakt auf Bedrohungen und Risiken hinweist. Pauschale Entfristungen von Gesetzen sind keine seriöse Evaluation. Das Evaluationsgebot gilt für Bundesgesetze, wie etwa für die Regelungen im Terrorismusbekämpfungsergänzungsgesetz (vgl. VIII. Tätigkeitsbericht, Nr. 24.1). Hier strebt die Bundesregierung eine Verlängerung um weitere 4 Jahre an, ohne vorherige gründliche unabhängige Evaluation, aber mit einer Ausweitung der Befugnisse des Verfassungsschutzes mittels Auskunftsrecht auch bei zentralen Stellen zu Konto- und Flugreisedaten (BR-Drs. 476/11). Das Evaluationsgebot gilt natürlich auch für Ländergesetze. Inhaltlich relevant sind u. a. die Auswirkungen von Maßnahmen auf Grundrechtspositionen unbeteiligter Dritter, die Wahrung des Kernbereichs privater Lebensgestaltung und verfahrens- und technikorientierte Schutzvorkehrungen (s. nochmals **Anlage 10**).

1.2 Nicht-öffentlicher Bereich

Initiativen der Bundesregierung im Datenschutz für die 17. Legislaturperiode des Deutschen Bundestags (ab 2009) betreffen den Beschäftigtendatenschutz, voraussichtlich die Stiftung Datenschutz, eventuell eine Regelung für Geodatendienste. Die grundlegende Novellierung des Datenschutzrechts wird auch mittelfristig kaum angegangen und umgesetzt. Abgewartet werden die beabsichtigten Maßgaben von Europäischer Ebene angesichts der von der Europäischen Kommission zunächst angestoßenen Überprüfung des allgemeinen Rechtsrahmens für den Datenschutz und einer Überarbeitung der Richtlinie 95/46/EG aus dem Jahre 1995 mittels eines im November 2010 für einen Konsultationsprozess vorgelegten Gesamtkonzepts (s. Nr. 3.1). Auch

sollen erst noch Ergebnisse der Enquete-Kommission des Deutschen Bundestages „Internet und digitale Gesellschaft“ vorliegen, die sich u. a. mit Themen des Urheberrechts, der Netzneutralität, des Datenschutzes und der Medienkompetenz befasst (vgl. BT-Drs. 17/5625).

Der Landesbeauftragte beteiligt sich auf verschiedene Weise an diesen rechts- und gesellschaftspolitischen Diskursen, so etwa über die Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Die Datenschutzkonferenz hat nach Vorarbeiten einer eigens gebildeten Arbeitsgruppe bei der Frühjahrskonferenz 2010 ein **Eckpunktepapier zur Modernisierung des Datenschutzrechts** mit vielen grundsätzlichen und konkreten Empfehlungen für eine neue verständliche Grundstruktur des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze als allgemeingültige Regelung mit Mindeststandards, Schutzzielen, technikneutralen Vorgaben unter Einbeziehung des Internets und Maßgaben für eine Stärkung der unabhängigen Datenschutzaufsicht beschlossen (s. Nr. 3.1). Die Vorschläge betreffen den nicht-öffentlichen und den öffentlichen Bereich.
In das Papier flossen auch Überlegungen einer Arbeitsgruppe ein, die sich mit „neuen Schutzzielen“ im Sinne eines proaktiven Datenschutzes durch Technik befasste (vgl. Rost/Bock, Privacy By Design und die Neuen Schutzziele, DuD 2011, 30).

Die Positionen der Konferenz werden vom Bundestag, so etwa in Entschließungen zu Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (zuletzt Entschließung vom 16. Dezember 2010, BT-Drs. 17/4179), und vom Bundesrat (Stellungnahme zum Gesetzentwurf der Bundesregierung, Beschluss vom 13. Februar 2009, Drs. 4/09, Nr. 32; Entschließung als Ergänzung zum Gesetzentwurf betr. Erfassung von Geodaten vom 9. Juli 2010, Drs. 259/10, Nr. 1, 3.1-3.13, 4; s. auch Beschluss einer Stellungnahme zum Gesamtkonzept für den Datenschutz in der Europäischen Union vom 11. Februar 2011, Drs. 707/10, Nr. 3; vgl. Nr. 3.1) unterstützt. Dagegen hat sich die Bundesregierung bislang reserviert gezeigt. Die Justizministerkonferenz sieht den Datenschutz als nicht wirksam geregelt an und verlangt mehr als ein schmales Gesetz zum umstrittenen Web-Dienst Google Street View. Das Ministerium des Innern des Landes Sachsen-Anhalt hat die Anregungen aus dem Eckpunktepapier positiv aufgenommen und bestätigt, dass das Datenschutzrecht internettauglich gemacht werden müsse, einhergehend mit einer Verständigung auf internationale Standards.

Interessant bei der Gesamtentwicklung und insbesondere bei der Befassung mit dem Regelungsbedarf für das oder im Internet ist die Erkenntnis, dass neben gesetzgeberischen Aktivitäten zunehmend auch auf **Selbstregulierungen der Wirtschaft**, bisweilen nur im Sinne ethischer Verpflichtungen, und zudem auf den Selbstdatenschutz des einzelnen Nutzers gesetzt wird. In einem Zwischenbericht der Enquete-Kommission des Bundestages findet sich die fragwürdige Aussage, dass „potenzielle Defizite staatlicher Aufsicht durch eine Einbindung der Unternehmen in die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden können“. Mit dem „Geodatenkodex“ liegt im Übrigen ein erster ausführlicher Selbstverpflichtungskanon vor (Nr. 3.1.3), der allerdings ein Handeln und Eingreifen des Gesetzgebers nicht entbehrlich macht und im Übrigen die Aufsichtsbehörden nicht unmittelbar bindet (vgl. auch § 38a BDSG). Bei den Datenskandalen

um die ohne Zustimmung der Nutzer erfolgte Speicherung von Aufenthaltsorten in Mobiltelefonen der Firma Apple und die Datenlecks und den Datenklau bei der Firma Sony wurde erneut ein Dilemma deutlich: Die großen Unternehmen agieren global, das Recht reagiert aber nur national, vielleicht noch europäisch. Und es läuft den technischen Entwicklungen mehr und mehr hinterher. Doch Verantwortung muss nicht nur ausgesprochen, sondern auch durchgesetzt werden. Insofern kommt es auf international verbindliche Standards an, die über das Safe Harbor Abkommen von 2000 zwischen der Europäischen Union und den USA hinausgehen. Danach erkennt die Kommission die Grundsätze des US-Handelsministeriums und zugleich die Angemessenheit des Datenschutzes bei US-Unternehmen, die sich an solche allgemeinen Datenschutzkriterien binden, an (vgl. auch **Anlage 37**).

Hinsichtlich der Betonung des Selbstschutzes, gefördert auch durch Maßnahmen der Medienkompetenzbildung, mag zunächst noch daran erinnert werden, dass das Bundesverfassungsgericht hinreichende Möglichkeiten für den Selbstdatenschutz für den Fall bejaht hat, dass sich Kommunikationsverbindungsdaten in der Einflusssphäre bzw. dem Herrschaftsbereich des Betroffenen befinden; ein unerwünschter Zugriff Dritter sei durch die Benutzung von Passwörtern und Verschlüsselungsprogrammen sowie Software zur Datenlöschung zu verhindern (BVerfGE 115, 166, 185f.). Doch ist dann eine oftmals übersehene Feststellung des Bundesverfassungsgerichts in dessen Entscheidung zur heimlichen Online-Überwachung vom 27. Februar 2008 relevant: „Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer und technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann.“ (BVerfGE 120, 274, 306). Selbstschutz ist schon bei den im eigenen Bereich des Nutzers erfolgenden Anwendungen kaum noch verlässlich möglich; unzumutbar und ungeeignet ist das bisherige Schutzprogramm etwa bei komplexen mobilen und allgegenwärtigen Datenverarbeitungen und auch bei Verarbeitungen in der „Wolke“ (vgl. Nrn. 1.3.2, 1.3.3). Daher sind Schutzmaßnahmen durch den Gesetzgeber bis hin zu voreingestellter datenschutzfreundlicher Technik („privacy by design“, „privacy by default“) zur Gewährleistung eines Systemdatenschutzes und Vermeidung von Gefährdungen der Persönlichkeit geboten. Gleichwohl bleibt die Mitwirkung der betroffenen Nutzer bei der Verinnerlichung und Ausübung des Prinzips der **Datensparsamkeit** unverzichtbar, aber eben nicht nur im Sinne technischer Grundkenntnisse, sondern einer kritikfähigen Grundhaltung. Dass man hierbei ebenfalls der Entwicklung hinterherläuft, macht die Notwendigkeit von Konzepten und Maßnahmen nicht entbehrlich (vgl. Nr. 21.2).

Solche Maßnahmen für den Selbstdatenschutz und vor allem zusätzlich eine Erweiterung und Stärkung der Position der Betroffenen, rechtlich wie technisch-organisatorisch, tragen mit dazu bei, den Betroffenen ihre Rechte der Kontrolle über die eigenen Daten tatsächlich zurückzugeben bzw. wirksam ausüben zu können. Auch hierzu finden sich in dem o. a. Eckpunktepapier der Datenschutzkonferenz mehrere Vorschläge, so zum Ausbau des Prinzips der **Transparenz**. Dieses bedarf einer wesentlichen Verstärkung. Transparenz der Datenverarbeitung schafft Vertrauen und Akzeptanz. Datenberge und heimliche Speicherungen, ob durch den Staat oder Unternehmen, bewirken das Gegenteil.

Damit wird zugleich der These widersprochen, den Selbstdatenschutz ausschließlich einer Selbstregulierung des Internets bzw. seinen Foren zu überlassen. Hinter dieser Sichtweise steckt auch der Gedanke der Informationsfreiheit des Internets, die eine Regulierung von außen verbiete. Wer so zu argumentieren versucht, verschiebt das Internet und seine Eingriffe auch in das reale Leben aber in einen rechtsfreien Raum; das gilt auch für den Bereich des Urheberrechts. Das Internet ist Chance, aber auch Risiko; der Staat hat aus seiner Schutzaufgabe heraus die Risiken zu mindern und einen Ausgleich der Grundrechte vorzunehmen. Die dem Staat obliegende Schutzpflicht, die das Rechtssystem, aber auch Bereiche von Technologieeinsatz und Medienbildung betrifft, erwächst aus dem Persönlichkeitsrecht (so auch BVerfG, Beschluss vom 23. Oktober 2006, 1 BvR 2027/02, DVBl. 2007, 111, s. IX. Tätigkeitsbericht, Nr. 1.2). Die von der „Post-Privacy“-Bewegung vertretene Auffassung, die Idee von Privatheit und Privatsphäre sei in der transparenten Internet-Gesellschaft überholt, trägt nicht, allerdings sind die Konzepte zu modernisieren.

Der Landesbeauftragte nahm Gelegenheit, die vorbeschriebenen Entwicklungen und Positionen im Ausschuss für Wirtschaft und Arbeit des Landtages darzustellen. Er bezieht die Überlegungen im Übrigen stets in seine Vorträge ein und äußert sich zu den vorerwähnten Aspekten in den Medien, unter Einbeziehung auch gesellschaftswissenschaftlicher Betrachtungen.

1.3 IuK-Technik und Organisation – Grundsatzthemen

Zu einer der ständigen Aufgaben des Landesbeauftragten zählt die Beobachtung der Entwicklung der Informations- und Kommunikationstechnologien (IuK, synonym auch IKT) und deren Bewertung aus der Sicht des Datenschutzes und der Datensicherheit. Dabei sind die rasant steigenden Teilnehmerzahlen im Internet und eine starkes Anwachsen internetbasierter Angebote und Services für Bürgerinnen und Bürger auffällig. Gefördert wird diese Entwicklung durch die erhöhte Verfügbarkeit von Breitbandanschlüssen für den Zugang zum Internet. Das Internet selbst durchdringt immer mehr Lebensbereiche der Bürgerinnen und Bürger und ist mittlerweile als fester Bestandteil von Geschäftsprozessen der Wirtschaft, aber auch von E-Government-Angeboten der öffentlichen Verwaltung, aus dem Alltag nicht mehr wegzudenken.

Für die Informationsgesellschaft selbst sind damit die sichere und verlässliche Funktion von IuK, die Informationssicherheit sowie die generelle Verfügbarkeit des Internets zu existenziellen Faktoren geworden. Das betrifft insbesondere die „Kritischen Infrastrukturen“ (KRITIS, s. IX. Tätigkeitsbericht, Nr. 1.3) von Wirtschaft und Verwaltung, aber auch Fragen der informationellen Selbstbestimmung bei der Nutzung des Internets selbst. Das Thema „Cybersicherheit“ hat damit für die Informationsgesellschaft des 21. Jahrhunderts neben „Cloud Computing“ eine herausragende Bedeutung erlangt.

Der Datenschutz und die Datensicherheit waren im zurückliegenden Berichtszeitraum so häufig Gegenstand öffentlicher Diskussionen und Debatten, besonders in den Medien. Als Stichworte seien hier beispielhaft Google Street View (s. Nr. 3.1.3), die Vorratsdatenspeicherung (s. Nr. 25.1), Cloud

Computing (s. Nr. 1.3.2), Mobile Computing (s. Nr. 1.3.3) und Open Government (s. Nr. 1.3.4) genannt.

Exemplarisch für neue Bedrohungsszenarien bei kritischen Infrastrukturen ist hier an den im Juli 2010 bekanntgewordenen Angriff einer Schadsoftware namens „Stuxnet“, die für Störungen in Anlagen des iranischen Atomprogramms entwickelt wurde, zu erinnern. Dabei handelte es sich beim sogenannten „Stuxnet-Wurm“ nach Ansicht der Fachwelt um das bis dato komplexeste Schadprogramm, das nahezu alle bisher bekannten Angriffsformen vereint.

In Fortsetzung ihrer Strategie zum Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung hat die Bundesregierung im Februar 2011 eine Cyber-Sicherheitsstrategie beschlossen. Kern dieser Strategie ist das neue „Nationale Cyber-Abwehrzentrum“, welches beim Bundesamt für die Sicherheit in der Informationstechnik (BSI) eingerichtet wurde. Damit soll die Information und operative Zusammenarbeit aller staatlichen Stellen optimiert und die Koordinierung von Schutz- und Abwehrmaßnahmen bei entsprechenden Vorfällen verbessert werden.

Das Internet vergisst nichts. Diese Erfahrung müssen immer mehr Internetnutzer machen, die Suchmaschinen wie „Google“, soziale Netzwerke wie „Facebook“, Webforen und Blogs oder auch Mikroblogging wie „Twitter“ nutzen. In der öffentlichen Debatte zur Möglichkeit der Löschung von Daten im Internet bzw. zur Sicherstellung der Herrschaft über die eigenen Daten im Internet wurde der Ruf nach einem „Digitalen Radiergummi“ laut, der in Anlehnung an den guten alten Radiergummi der „offline-Welt“ solche Probleme lösen sollte. Der unter dem Slogan „Digitaler Radiergummi“ mit Unterstützung der Politik vorgestellte durchaus lobenswerte Ansatz, bekannt geworden als Browser-Plugin „X-pire!“, hielt aber einer kritischen Auseinandersetzung mit seiner Wirksamkeit nicht stand. Mittels X-pire! sollen Bilder vor dem Hochladen ins Internet mit einem Verfallsdatum versehen und damit zeitlich begrenzt zugänglich gemacht werden. Allerdings ist dies allein nur mit einer Softwarelösung nicht möglich. Diese Meinung wird auch vom Landesbeauftragten geteilt. Der gewissenhafte und sparsame Umgang mit den eigenen Daten im Internet ist gegenwärtig immer noch die wichtigste Voraussetzung für den Schutz der eigenen Privatsphäre.

Mit dem neuen Artikel **91c Grundgesetz** (GG) hat der Gesetzgeber eine verfassungsrechtliche Grundlage für die Zusammenarbeit von Bund und Ländern bei Planung, Errichtung und Betrieb ihrer informationstechnischen Systeme geschaffen sowie dem Bund die Zuständigkeit für ein Verbindungsnetz übertragen. Mit der Bildung des IT-Planungsrats wurde auf organisatorischer Ebene in Zusammenarbeit zwischen Bund, Ländern und Kommunen ein völlig neuer Weg beschritten. Inwieweit dieses Gremium auch die Belange des Datenschutzes und der Datensicherheit, insbesondere die Belange der Länder, ausreichend berücksichtigt, muss nach der bisherigen Erfahrung des Landesbeauftragten mit einer gewissen Skepsis betrachtet werden (s. Nr. 1.3.1).

1.3.1 IT-Planungsrat – eine Zwischenbilanz

Der Landesbeauftragte hat in seinem IX. Tätigkeitsbericht (Nr. 1.3) über die Beschlüsse der Föderalismuskommission II (5. März 2009) und die damit verbundene Einführung des neuen **Artikel 91c GG** berichtet, der am 1. August 2009 in Kraft trat. Unter dem bekannten Begriff „IT ins Grundgesetz“ wurde damit erstmals ein verfassungsrechtlicher Rahmen für diese Kooperation von Bund und Ländern geschaffen. Er ermöglicht Bund und Ländern, bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgaben notwendigen informationstechnischen Systeme zusammenzuarbeiten. Hierzu können Bund und Länder die dafür notwendigen Standards und Sicherheitsanforderungen festlegen. Darüber hinaus können die Länder den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren. Abschließend erhält der Bund die ausschließliche Kompetenz zur Errichtung und zum Betrieb eines **Verbindungsnetzes** zwischen den informationstechnischen Netzen des Bundes und der Länder auf der Grundlage eines Bundesgesetzes mit Zustimmung des Bundesrates.

Mit dem am 18. August 2009 in Kraft getretenen Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des GG – **IT-NetzG** (Artikel 4 des Begleitgesetzes zur zweiten Föderalismusreform vom 10. August 2009, BGBl. I S. 2072) wurde diese Zuständigkeit des Bundes gesetzlich verankert. Allerdings tritt § 3 des IT-NetzG, der den Datenaustausch zwischen Bund und den Ländern über das Verbindungsnetz regelt, erst mit dem 1. Januar 2015 in Kraft.

Die bisher vom Deutschland-Online Infrastruktur e.V. (DOI-Netz e.V.) wahrgenommenen Aufgaben wurden zum 31. Dezember 2010 dem Bund übertragen. Die Verantwortung für den operativen Betrieb des Verbindungsnetzes trägt seit dem 1. Januar 2011 die Bundesstelle für Informationstechnologien im Bundesverwaltungsamt. Die strategischen Aufgaben werden durch das Bundesministerium des Innern wahrgenommen.

Am 1. April 2010 trat der sogenannte **IT-Staatsvertrag** (Gesetz zum Vertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in der Verwaltung von Bund und Ländern vom 27. Mai 2010) nach vorausgegangener Ratifizierung durch alle Bundesländer in Kraft (BGBl. I S. 662). Sachsen-Anhalt stimmte diesem Staatsvertrag mit Gesetz vom 23. März 2010 (GVBl. LSA S. 142) zu. Der IT-Staatsvertrag bildet die Grundlage für die Arbeitsweise des IT-Planungsrates (IT-PLR). Demnach hat der IT-PLR folgende wesentliche Aufgaben:

- Koordination der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik,
- Beschlussfassung über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards,

- Projektsteuerung zu Fragen des informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens (E-Government-Projekte), die dem IT-PLR zugewiesen werden,

- Koordinationsgremium nach Maßgabe des Gesetzes zur Ausführung von Artikel 91c Abs. 4 GG – (IT-NetzG).

Die konstituierende Sitzung des IT-PLR erfolgte am 22. April 2010 in Berlin. Die 4. Sitzung des IT-PLR fand am 3. März 2011 anlässlich der CeBIT in Hannover erstmals unter Ländervorsitz (Baden-Württemberg) statt. Dem IT-PLR gehören als Mitglieder die Beauftragte der Bundesregierung für Informationstechnik sowie je ein für Informationstechnik zuständiger Vertreter jedes Landes an. Beratende Teilnehmer an den Sitzungen sind drei Vertreter der Kommunalen Spitzenverbände auf Bundesebene sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Die Nichtberücksichtigung eines Vertreters der Datenschutzbeauftragten der Länder zur beratenden Teilnahme war angesichts der Themen des IT-PLR (Sicherheitsstandards, Verbindungsnetz, E-Government-Projekte), welche auch gerade Datenschutzfragen der Länder unmittelbar berühren, unverständlich.

Gerade diese ständige Einbeziehung in die Sitzungen des IT-PLR war u. a. eine der Forderungen einer Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009 zu diesem IT-Staatsvertrag (**Anlage 2**).

Mit Unterstützung verschiedener Landesparlamente, in Sachsen-Anhalt durch einen Beschluss des Landtages vom 18. März 2010 (LT-Drs. 5/73/2508 B), wurden die Landesregierungen aufgefordert, für eine entsprechende Änderung der Geschäftsordnung des IT-PLR einzutreten und damit die ständige beratende Teilnahme eines Vertreters der Datenschutzbeauftragten der Länder zu ermöglichen.

Nach diesen Interventionen wurde die vom IT-PLR verabschiedete **Geschäftsordnung** in § 6 Abs. 3 dahingehend ergänzt, dass zusätzlich ein Vertreter der Datenschutzbeauftragten der Länder an den Sitzungen teilnehmen darf, sofern die Länder betreffende datenschutzrelevante Belange erörtert werden. Diese Regelung entspricht nicht ganz der Forderung nach einer regelmäßigen Einbindung der Datenschutzbeauftragten der Länder, sollte aber, da die Mehrzahl der zu beratenden Themen einen Datenschutzbezug für die Länder besitzt, in der Praxis nicht weiter hinderlich sein.

Die Aufgabe des Länder-Vertreters nimmt der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wahr, der gleichzeitig auch Vorsitzender des Arbeitskreises technische und organisatorische Datenschutzfragen ist.

In Sachsen-Anhalt hat die Staatskanzlei allerdings für eine regelmäßige Beteiligung des Landesbeauftragten Sorge getragen. Dazu wurde die Geschäftsordnung des Ständigen Staatssekretärsausschusses „Informationstechnologie“ entsprechend ergänzt. Der Landesbeauftragte sowie auch die

Vertreter der Kommunalen Spitzenverbände nahmen danach an den vorbereitenden Sitzungen des Staatssekretärsausschusses für den IT-PLR beratend teil. Zukünftig ist der IT-Beauftragte der Landesregierung im Finanzministerium der zuständige Ansprechpartner (vgl. Nr. 4.3).

So weit, so gut könnte man nun denken, kritisch angemerkt an dieser Stelle seien aber die bis zur 4. Sitzung sehr formalistische Vorbereitung der Tagesordnungspunkte durch die Geschäftsstelle des IT-PLR in sogenannten „Steckbriefen zur Themenanmeldung“ sowie der sehr enge Zeitrahmen für die Vorbereitung der bisherigen Sitzungen des IT-PLR. Nicht selten wurde die datenschutzrechtliche Relevanz von Tagesordnungspunkten nicht erkannt.

Aus diesem Grund erscheint es dem Landesbeauftragten notwendig, in einem weiteren Beitrag (Nr. 4.2) auf einige datenschutzrelevante Vorhaben des IT-PLR hinzuweisen, welche auch eine Bedeutung für Sachsen-Anhalt haben. In den vorbereitenden Sitzungen des Staatssekretärsausschusses bestand zudem für den Landesbeauftragten, natürlich auch aus praktischen und zeitlichen Gründen, kaum die Möglichkeit einer vertieften Diskussion bzw. Erörterung von datenschutzrelevanten Einzelthemen der Tagesordnung.

Gleichzeitig ist damit die Aufforderung an die betroffenen Ressorts verbunden, unabhängig von der Geschäftsordnung der Landesregierung, ihrer rechtzeitigen Unterrichtungspflicht gem. § 14 Abs. 1 Satz 2 DSG-LSA nachzukommen. Diese verpflichtet bei grundlegenden Planungen des Landes zum Aufbau bzw. zur Änderung von Vorhaben zur automatisierten Verarbeitung personenbezogener Daten zur rechtzeitigen Unterrichtung des Landesbeauftragten bereits im **Planungsstadium**. Dieser Umstand trifft sicherlich für den überwiegenden Teil der Vorhaben, insbesondere die zukünftige E-Government-Strategie des Landes Sachsen-Anhalt zu, die sich an der Nationalen E-Government-Strategie ausrichten und wie diese einen Zeithorizont bis zum Jahr 2015 umfassen soll.

1.3.2 Cloud Computing – virtuelle „Rechnerwolke“

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 1.3) auf den sich abzeichnenden Paradigmenwechsel beim Einsatz der Informations- und Kommunikationstechnik (IuK) bzw. der Informationsverarbeitung durch Nutzung internetbasierter Dienste unter dem damals neuen Schlagwort „Cloud Computing“ hingewiesen. Große Internet-Unternehmen wie Amazon, Google oder Microsoft stellen mittlerweile potentiellen Nutzern IT-Ressourcen (ganze Entwicklungs-Plattformen, Infrastrukturen und Software) als IT-Dienstleistungen auf Mietbasis über das Internet zur Verfügung. Damit soll den Kunden die Konzentration auf ihr sogenanntes Kerngeschäft erleichtert werden, weil damit ein Großteil der sonst durch sie selbst zu betreibenden und zu unterhaltenden IT-Ressourcen überflüssig werden.
Aus wirtschaftlicher Sicht versprechen die Anbieter und Befürworter des Cloud Computing den Nutzern bzw. Kunden neben einem möglichen weltweit verfügbarem Zugriff auf diese IT-Ressourcen insbesondere eine enorme Kosteneinsparung, eine hohe Flexibilität bei der Bereitstellung sowie eine schnelle und dynamische Anpassung der benötigten IT-Ressourcen, ob es

nun um Bandbreite, Speicherkapazität (Daten- und Arbeitsspeicher) oder Rechenleistung geht.

So wie heutzutage von jedermann Strom aus der Steckdose bezogen werden kann und nur das bezahlt werden muss, was man verbraucht, soll jedermann IT-Dienstleistungen aus der „Rechnerwolke“ über das Internet beziehen können. Datenbanken, Fach-Anwendungen, Server oder Webservices – es gibt gegenwärtig beim Thema Informationsverarbeitung fast nichts, was nicht auch in einer Cloud genutzt werden könnte.

Natürlich ist damit die Anwendung von Cloud Computing auch für die öffentliche Verwaltung gerade unter dem Aspekt der Verwaltungsmodernisierung (Kosteneinsparung und Effizienzsteigerung beim Einsatz von IuK) ein aktuelles Thema geworden, ob nun als öffentliche Stelle in der Rolle des Nutzers von Cloud-Diensten oder der eines zentralen IT-Dienstleisters in einem Land als Anbieter von Cloud-Diensten. Aus datenschutzrechtlicher Sicht bleibt aber ein zentrales Problem des Cloud Computing das Thema der Datensicherheit und hier insbesondere die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit sowie die Revisionssicherheit bei der Verarbeitung personenbezogener Daten. Weitere Erläuterungen zum Thema Cloud Computing und Datenschutz werden in Nr. 14.1 dieses Tätigkeitsberichts gegeben.

1.3.3 Mobile Computing

Seit einigen Jahren bereits entwickeln sich Mobiltelefone immer mehr zu Mini-PCs, sogenannten „Smartphones“, welche eine allumfassende Vernetzung mit dem Internet aufweisen und so ein wesentliches Werkzeug zur Nutzung von Netzdiensten und Angeboten sowohl der Privatwirtschaft als auch des E-Government und Angeboten öffentlicher Stellen darstellen. Erkennbar sind hierbei eine rasante Steigerung der Verbreitung solcher Geräte, aber auch der Datenvolumina, und eine stetige Vernetzung von öffentlichen und nichtöffentlichen Diensten.

Zuletzt durch die Aufdeckung und das Bekanntwerden der heimlichen Aufzeichnung geografischer Ortungsdaten von WLAN- und Mobilfunkzellen in Verbindung mit Zeitstempeln in einer entsprechenden Datenbank beim beliebten „iPhone“ und dem „iPad“ der Firma Apple im April 2011 wurde die Öffentlichkeit wieder einmal mit Defiziten beim Datenschutz konfrontiert, die den privaten Nutzern nicht bekannt bzw. bewusst waren. Diese sogenannte Ortungsfunktion dient Apple bei seinem Betriebssystem „iOS“ eventuell schon länger zur unverschlüsselten Aufzeichnung von Ortungsdaten und damit der Pflege dieser bisher scheinbar unbekannten Datenbank in den Smartphones selbst. Ähnliche Anwendungsszenarien sind auch bei den Mitbewerbern wie Google mit dem Betriebssystem „Android“ und Microsoft mit dem Betriebssystem „Windows Phone 7“ im heiß umkämpften Markt dieser mobilen „Alleskönner“ zu vermuten.

Ob es sich hier bei Apple um einen schlichten Programmierfehler handelte oder die Speicherung in der Datenbank u. a. zur Vorbereitung der Nutzung zukünftiger Dienste dienen könnte (z. B. Aufbau einer Verkehrsdatenbank für Staumeldungen), wurde in Fachkreisen kontrovers diskutiert. Auf ihrer Inter-

netseite nahm die Firma Apple zu den Vorwürfen, dass das iPhone und das iPad vermeintlich Bewegungsprofile von Nutzern aufzeichnen würde, Stellung. Defizite bei Datenschutz und Transparenz für den Nutzer wurden dabei eingeräumt. Apple sprach bezüglich der Fortschreibung dieser Datenbank – fast wie immer in solchen Fällen üblich – von einem Softwarefehler. Auch wenn sich mittels dieser Datenbank kein komplettes Bewegungsprofil eines Nutzers erstellen lässt, beabsichtigt die Firma Apple mit einem Update des Betriebssystems diesen Softwarefehler zu beheben und das Backup dieser Ortungsdatenbank auf dem PC des Nutzers nicht mehr zu ermöglichen. Zukünftig soll die Datenbank auf die Ortungseinträge der letzten sieben Tage beschränkt und beim Ausschalten des Ortungsdienstes komplett gelöscht werden. Zudem soll mit einem nachfolgenden größeren Update des Betriebssystems „iOS“ diese Datenbank auf dem iPhone zusätzlich verschlüsselt werden.

Eventuell geplanten Einsatzszenarien für Smartphones durch öffentliche Stellen sollte deshalb auch eine Gefährdungs- und Risikoanalyse vorausgehen, um eine datenschutzgerechte Nutzung zu gewährleisten.

Mobile Geräte werden zusätzlich zu den beschriebenen auch von weiteren Risiken und Angriffsszenarien bedroht, sodass in diesem Tätigkeitsbericht das Thema aufgegriffen wird (s. Nr. 14.3).

1.3.4 Open Government / Open Data

Der Begriff „Open Government“ umschreibt allgemein Initiativen und Maßnahmen mit dem Ziel der Öffnung von Staat und Verwaltung gegenüber allen gesellschaftlichen Gruppen (Wirtschaft, Bürgerinnen und Bürgern). Open Government gliedert sich dabei in drei wesentliche Themenbereiche:

- **Transparenz** (Offenlegung der Entscheidungen und Prozesse von Staat und Verwaltung sowie öffentliche Verfügbarkeit dieser Daten),
- **Partizipation** (Mitwirkungsmöglichkeiten der Allgemeinheit an staatlichen Entscheidungsprozessen),
- **Kooperation** bzw**.** Kollaboration (Zusammenarbeit zwischen staatlichen und gesellschaftlichen Gruppen).

Der Begriff „Open Data“ umfasst allgemein die vorhandenen Datenbestände des öffentlichen Sektors (insbesondere der öffentlichen Verwaltung), die durch ihre elektronische Bereitstellung der Allgemeinheit mit gewissen Einschränkungen (insbesondere unter Beachtung des Datenschutzes sowie von Betriebs- und Geschäftsgeheimnissen) zur Nutzung und Weiterverwendung zur Verfügung gestellt werden.

Die Umsetzung der Open Government-Strategie soll dabei den gesellschaftlichen Zusammenhalt fördern, die Glaubwürdigkeit des poltischen Handelns stärken, neue Geschäftsmodelle für die Wirtschaft erschließen und nicht zuletzt auch die Qualität und die Effizienz der öffentlichen Verwaltung erhöhen.

Nach den Zielvorstellungen im Regierungsprogramm „Vernetzte und transparente Verwaltung“, beschlossen vom Bundeskabinett am 18. August 2010, ist für das Projekt Open Government die Abstimmung einer gemeinsamen Strategie mit den Ländern bis 2012 und für 2013 die Umsetzung dieser gemeinsamen Strategie geplant.

Die vom IT-Planungsrat am 13. September 2010 verabschiedete Nationale E-Government-Strategie hat hierzu den Themengebieten Transparenz, Datenschutz und Datensicherheit (Zielbereich C) sowie gesellschaftliche Teilhabe (Zielbereich D) zwei wesentliche Zielbereiche gewidmet.

In der „Dresdner Vereinbarung“ wird diese Zielstellung des Regierungsprogramms aufgenommen. Die Bundesregierung vereinbarte gemeinsam mit Verwaltung, Wirtschaft und Wissenschaft auf dem 5. IT-Gipfel am 7. Dezember 2010 in Dresden das ehrgeizige Ziel, im Rahmen des Open Government bis zum Jahr 2013 eine zentrale Open Data-Plattform aufzubauen. Sie soll die Plattformen von Bund, Ländern und Kommunen vernetzen und einen Beitrag zum Zugang zu Daten und Informationen der öffentlichen Verwaltung sowie zum weiteren Ausbau des prozessorientierten und ebenenübergreifenden E-Governments leisten.

Die Senatorin für Finanzen der Freien Hansestadt Bremen, das Institut für Informationsmanagement Bremen und die Landesbeauftragte für Datenschutz und Informationsfreiheit haben aufgrund ihrer Erfahrungen mit dem Informationsregister Bremen in der Bremer Empfehlung zu Open Government bereits konkrete Vorschläge unterbreitet, welche Maßnahmen bei der Entwicklung einer solchen Open Data-Plattform berücksichtigt werden sollten.

Da bei der Umsetzung dieser Open Government-Strategie auf der Basis einer Open Data-Plattform Datenschutz und Informationsfreiheit Hand in Hand gehen, ist die aktive Einbeziehung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz und die Informationsfreiheit wünschenswert. Insbesondere wird es im Wesentlichen darauf ankommen, den Belangen der Informationsfreiheit unter Beachtung des Datenschutzes Rechnung zu tragen. Unter diesem Aspekt wird der Landesbeauftragte die weitere Entwicklung auf Bundes- wie Landesebene beobachten und die Ressorts beratend unterstützen. Das Thema wird auch Gegenstand des II. Tätigkeitsberichts zur Informationsfreiheit sein.

1.4 Zusammenfassung und Ausblick

Wesentliche Aussagen aus den vorangegangenen Bemerkungen lauten:

- Verbot der Totalüberwachung – Evaluation vorhandener Überwachungen,
- Verbot der Registrierung und Katalogisierung der Persönlichkeit – Verbot der Erstellung von Persönlichkeitsprofilen,
- Datenschutz als präventiver Schutz gegen Gefährdungen der informationellen Selbstbestimmung als Teil der Persönlichkeit – Notwendigkeit vertrauensbildender Maßnahmen des Staates,

- Informationelle Selbstbestimmung als Funktionsbedingung der freiheitlichen Demokratie,

- Notwendigkeit der grundlegenden Novellierung des Datenschutzrechts insbesondere im Hinblick auf die Entwicklungen durch das und im Internet.

Herausragende Gerichtsentscheidungen im Berichtszeitraum (vgl. daneben auch VIII. Tätigkeitsbericht, Nr. 1.1, und IX. Tätigkeitsbericht, Nr. 1.4) waren:

- Urteil des Bundesverfassungsgerichts vom 2. März 2010 – 1 BvR 256/08 u. a. – zur Vorratsspeicherung von Telekommunikationsverkehrsdaten

- Urteil des Bundesverwaltungsgerichts vom 21. Juli 2010 – 6 C 22/09 – zur Beobachtung von Abgeordneten durch den Verfassungsschutz (NVwZ 2011, 161; Fortsetzung vor dem Bundesverfassungsgericht – kritische Anmerkungen bereits bei Klatt, NVwZ 2011, 146; vgl. auch Beschluss des Bundesverfassungsgerichts vom 1. Juli 2009 – 2 BvE 5/06 – zum Auskunftsrecht für Abgeordnete über nachrichtendienstliche Beobachtungen von Abgeordneten)

- Urteil des Bundesarbeitsgerichts vom 16. November 2010 – AZR 573/09 – zum Einsichtsrecht in die Personalakte nach Beendigung des Arbeitsverhältnisses (NJW 2011, 1306)

Daneben ist das Urteil des Europäischen Gerichtshofs vom 9. März 2010 - C 518/07 – (NJW 2010, 1265) zur Unabhängigkeit der Datenschutzaufsicht von besonderer Bedeutung (s. Nr. 3.2).

Gegenwart und Zukunft des Datenschutzes werden auch in der Entschließung der Datenschutzkonferenz vom 8./9. Oktober 2009 treffend beschrieben:

Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- *das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;*

- *die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;*

- *ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;*

- *die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;*

- *die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;*

- *auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;*

- *im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;*

- *die Videoüberwachung in Staat und Gesellschaft einzuschränken;*

- *den Schutz der Meldedaten zu verbessern;*

- *ein praktikables Datenschutzaudit zu schaffen;*

- *die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.*

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

2 Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Geschäftsstelle

Die Anzahl der Geschäftseingänge ist weiter gestiegen:
2009: 4.045 2010: 4.109 (2007: 3.350, 2008: 3.730)

Insgesamt wurden in 2009/2010 2.950 schriftliche Äußerungen (Stellungnahmen, Antworten etc.) verfasst (2007/2008: 2.300). Darunter befanden sich 138 Petentenfälle (2007/2008: 111).

Eingänge aus dem nicht-öffentlichen Bereich – Beschwerden, Presseanfragen, Einladungen zu Tagungen und Vorträgen – nahmen zu.

Kontrollen wurden anlassabhängig und anlassunabhängig durchgeführt: Unter besonderer Aufmerksamkeit und einem hohen Zeitaufwand standen die Vorbereitung und die Kontrolle der Justizvollzugsanstalt Burg, bei der im Kern zu klären war, inwieweit öffentliche Aufgaben im Rahmen der Auftragsvergabe durch Private übernommen werden durften. Weitere Prüfungsschwerpunkte waren die Überprüfung der Datenarchivierung der Polizeidirektion Sachsen-Anhalt Ost im Rahmen der sogenannten „Dessauer Staatsschutzaffäre“, welche ebenfalls einen hohen zeitlichen und personellen Einsatz bedingte. Kontrollen wurden u. a. in einigen Kommunen im Rahmen von Querschnittsprüfungen durchgeführt. Geprüft wurden auch eine Ausländerbehörde, Vollzugspolizeidienststellen sowie die Beschwerdestelle der Polizei, zwei Kfz-Zulassungs- und Fahrerlaubnisbehörden zur Thematik Steuerrückständedatei, Kfz-Zulassungsvoraussetzung, Online-Anbindung und Datenabgleich mit dem Kraftfahrtbundesamt, zwei Personalämter, ein Gymnasium und eine berufsbildende Schule, drei Personalausweisbehörden im Zusammenhang mit der Ausgabe des elektronischen Reisepasses, mehrere Arbeitsgemeinschaften und Optionskommunen nach dem Sozialgesetzbuch II und das Statistische Landesamt zur Vorbereitung und Umsetzung des Zensus 2011. Desweiteren wurden Vorgänge mit datenschutzrechtlicher Aktualität bei einigen kommunalen Schiedsstellen begutachtet. Im Bereich einer Waffenbehörde wurde ein Abrufverfahren unter Datenschutzaspekten beleuchtet. Der Holzverkauf und die Privatwaldverwaltung waren Anlass zur Kontrolle bei einigen Forstämtern. Weitere technisch-organisatorische Prüfungsschwerpunkte waren die Umsetzung der Fahrererlaubnisprüfung am PC, der VDV-Kernapplikationen zum eTicketing bei einem Nahverkehrsunternehmen sowie die praktische Umsetzung von SALSA (Secure Access Land Sachsen-Anhalt) beim Technischen Polizeiamt sowie der PKI LSA (Public Key Infrastruktur Land Sachsen-Anhalt).

Informationsbesuche erfolgten u. a. zur Umsetzung und zum Aufbau eines D115-konformen, telefonischen Service Centers in Sachsen-Anhalt und zur Frage der Geodatenverarbeitung im eigenen Wirkungskreis der Kommunen. Weitere Informationsbesuche fanden in der Universitätsklinik Magdeburg zum Neugeborenen-Screening, in einem Gesundheitsamt, beim „Einheitlichen Ansprechpartner“ (EA) im Landesverwaltungsamt zur Umsetzung der EG-Dienstleistungsrichtlinie und deren technischer Realisierung im Landes-

rechenzentrum sowie in der Polizeidirektion Sachsen-Anhalt Süd zur sogenannten Rasterfahndung Ermittlungsgruppe „Schulweg“ statt. Die Einführung des neuen Personalausweises (nPA) war Anlass, einzelne im Jahr 2010 an der Feldtestphase beteiligte Kommunen aufzusuchen und deren Umsetzung anhand praktischer Fälle zu begleiten.

Die Erfahrungsaustausche mit den behördlichen Datenschutzbeauftragten der Landkreise und kreisfreien Städte wurden fortgesetzt (vgl. IX. Tätigkeitsbericht, Nr. 2.1).

Der Öffentlichkeitsarbeit wurde weiterhin besonderes Augenmerk geschenkt, mittels ständiger Aktualisierung des Angebots auf der Homepage, Pressemitteilungen, Interviews und Hinweisen (vgl. auch Nr. 2.4).

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

Eine große Herausforderung stellte der Umzug der Geschäftsstelle im August 2009 von dem seit 1992 genutzten Gebäude in der Berliner Chaussee 9 ins Zentrum in die Leiterstraße 9 dar. Die neuen Verwaltungsräume sind angemessen und die Geschäftsstelle profitiert auch von der Nähe zu Landtag und Landtagsverwaltung.

Das Ausscheiden des Referatsleiters des Referats 1 und Leiters der Geschäftsstelle im Februar 2010 – faktisch war die Position schon seit November 2009 vakant – und ein langwieriges Auswahl- und Nachbesetzungsverfahren führten zu Mehrbelastungen und hatten auch zur Folge, dass nicht alle geplanten Vorhaben ganz und gar umgesetzt werden konnten. Die Stelle konnte erst zum 16. Mai 2011 nachbesetzt werden.
Das aktuelle Organigramm der Geschäftsstelle ist beigefügt (**Anlage 38**).

Der Landesbeauftragte selbst wurde auf Vorschlag der Landesregierung am 9. Dezember 2010 vom Landtag für eine zweite Amtsperiode wiedergewählt, die am 16. März 2011 begann.

Mit der vorgesehenen Übertragung der zusätzlichen Aufgabe der Aufsicht über den nicht-öffentlichen Bereich (vgl. Nr. 3.2) wird eine personelle und sächliche Mehrausstattung der Geschäftsstelle unumgänglich werden.

Datenschutzmanagement

Eine besondere Initiative im Berichtszeitraum betraf im Jahre 2010 Querschnittskontrollen in Kommunen, d. h. die Prüfung in mehreren Fachbereichen nebst Gesprächen mit Behördenleitung und behördlichem Datenschutzbeauftragten. Daran schloss sich im März 2011 die Veröffentlichung einer Broschüre zum Datenschutzmanagement, die den Landes- und Kommunalbehörden zur Verfügung gestellt wurde, an.

Der Landesbeauftragte hat bei Kontrollen immer wieder festgestellt, dass bei den Behörden defizitäre Kenntnisse über Grundsätze, Verfahren und Organisation des Datenschutzes bestehen, mit der Folge, dass die Umsetzung von Maßgaben des Datenschutzes und der Datensicherheit nur unzureichend gelingt. Oftmals wird für den Datenschutz allein der behördliche Datenschutz-

beauftragte verantwortlich gemacht, der mangels Zeit und wegen anderer Aufgaben in der Behörde regelmäßig überlastet ist. Dies gilt auch für das Erstellen und Vorhalten eines aktuellen Verfahrensverzeichnisses mit Angaben über die automatisierten Datenverarbeitungen der Behörde (§ 14 Abs. 3 DSG-LSA). Die Aufgabe des Datenschutzbeauftragten besteht vornehmlich in einer Mitwirkung und behördeninternen Selbstkontrolle, die Hauptverantwortung für die Einhaltung datenschutzrechtlicher Vorschriften trägt die Behördenleitung (§ 14 Abs. 1 DSG-LSA); daneben ist jeder Beschäftigte selbst mitverantwortlich (§ 5 Satz 1 DSG-LSA).

In der Broschüre, die auch über die Homepage des Landesbeauftragten abrufbar ist, werden verfassungsrechtliche Grundsätze des Datenschutzes, datenschutzrechtliche Grundsätze, Betroffenenrechte sowie Inhalte und Verfahren eines Datenschutzmanagements in Theorie und Behördenalltag dargestellt. Ein besonderer Aspekt betrifft Risiken für die Datensicherheit und die dagegen wirkenden technischen und organisatorischen Schutzmaßnahmen. Zur Thematik sind Fortbildungen für die Landes- und Kommunalbehörden vorgesehen. Die Orientierungshilfe wurde in das Internetangebot des Städte- und Gemeindebundes Sachsen-Anhalt aufgenommen.

2.2 Schwerpunkte – Empfehlungen

Wichtige Einzelvorgänge im Berichtszeitraum betrafen:

- Datei DOMEA beim Verfassungsschutz (Nr. 26.2),
- Datenarchivierung bei der PD Ost (Nr. 19.1),
- Prüfung der Aufwandsentschädigungen der Abgeordneten durch den Landesrechnungshof (Nr. 17.1),
- JVA Burg (Nrn. 24.1, 24.2),
- Zensus 2011 (Nr. 23.1).

Längerfristige Vorhaben betreffen:

- Modernisierung des Datenschutzrechts (Nr. 3.1 und 3.2),
- Datenschutzmanagement (Nr. 2.1),
- Medienkompetenz (Nr. 21.2),
- IT-Strategie und E-Government, IT-Planungsrat (Nrn. 4.1 ff.).

Die Mitwirkung an besonderen Gesetzgebungsverfahren erfolgte insbesondere bei folgenden Landesgesetzen:

- Umsetzung der EU-Dienstleistungsrichtlinie (Nr. 4.6),

- Maßregelvollzugsgesetz (Nr. 12.4),

- Stärkung der Datenschutzaufsicht – Übertragung der Datenschutzkontrolle für den nicht-öffentlichen Bereich auf den Landesbeauftragten (Nr. 3.2).

Empfehlungen und Forderungen für das Land Sachsen-Anhalt
(unberührt bleiben die Hinweise, Maßgaben und Empfehlungen unter den Einzelbeiträgen dieses Berichts)

1. Stärkung des Datenschutzbewusstseins in den Behörden mittels eines umfassenden Datenschutzmanagements (Nr. 2.1),

2. Modernisierung des DSG-LSA im Hinblick auf materielle Regelungen (Nr. 3.1.1),

3. Stärkung des Verbraucherdatenschutzes insbesondere durch die Zusammenfassung von Zuständigkeiten und Schaffung eines Ansprechpartners innerhalb der Landesregierung,

4. Intensivierung der Umsetzung des Konzepts der Landesregierung (Kultusministerium) zur Medienkompetenzbildung (Nr. 21.2),

5. Anpassung der IT-Strategie des Landes und Fortschreibung des E-Government-Maßnahmenplanes (Nrn. 4.1, 4.4)

6. Anpassung des SOG LSA an die Vorgaben des Bundesverfassungsgerichts (Nr. 19.2),

7. Beschränkung der Datenverarbeitung durch private Dienstleister in der Justizvollzugsanstalt Burg – Vorlage eines Datenschutzkonzepts (Nrn. 24.1, 24.2).

2.3 Zusammenarbeit mit anderen Institutionen

Infolge von Beratungsaufgaben in der Gesetzgebung wie auch bei mehreren Einzelvorgängen ergaben sich viele Kontakte mit dem **Landtag** bzw. seinen Ausschüssen.

Der Landesbeauftragte kann sich eine weitere Verstärkung von Datenschutzaspekten in Positionen des Landtages vorstellen. Positiv hervorzuheben ist der Beschluss des Landtages vom 3. Februar 2011 (LT-Drs. 5/88/3072 B) und das darin geäußerte Bekenntnis für einen konsequenten Datenschutz im öffentlichen wie nicht-öffentlichen Bereich mit einer unabhängigen Aufsicht (vgl. Nr. 3.2). Eine effektive Regelung erwartet der Landtag auch für den Beschäftigtendatenschutz.

Die Zusammenarbeit auch mit den Fraktionen wurde vom Landesbeauftragten weiter gepflegt. Mit einer beim Landesbeauftragten einzurichtenden Datenschutzkommission, in Anlehnung an Vorbilder in anderen Ländern vom

Landesbeauftragten seit längerem erwogen, könnte die Zusammenarbeit auch institutionell weiter verstetigt werden (vgl. Nr. 3.2).

Mit **Landtagspräsident** Steinecke und der **Landtagsverwaltung** wurde die vertrauensvolle Zusammenarbeit der vergangenen Jahre fortgesetzt. Mit dem neuen Landtagspräsidenten der 6. Wahlperiode, Detlef Gürth, wurde daran angeknüpft. Die Landtagsverwaltung unterstützte den Landesbeauftragten weiterhin in Personalangelegenheiten und Haushaltsbelangen (vgl. § 21 Abs. 3 DSG-LSA); vgl. auch Nr. 3.2. Der Landesbeauftragte wurde auch in einem konkreten Vorgang betreffend die Prüfung von Abgeordnetenentschädigungen durch den Landesrechnungshof mittels Unterlagen und Stellungnahmen der Landtagsverwaltung unterstützt (s. Nr. 17.1).

Ministerpräsident Prof. Dr. Wolfgang Böhmer besuchte die Geschäftsstelle am 16. Dezember 2010.

Die Landesministerien und Behörden der Landes- wie der Kommunalverwaltung nahmen die Beratung des Landesbeauftragten weiter intensiv in Anspruch.

Mit den **Aufsichtsbehörden für den nicht-öffentlichen Bereich,** dem Ministerium des Innern und dem Landesverwaltungsamt, bestand weiterhin Kontakt, auch im Rahmen alljährlicher Erfahrungsaustausche auf Einladung des Landesbeauftragten. Das Landesverwaltungsamt legte seinen vierten Tätigkeitsbericht für den Zeitraum 1. Juni 2007 bis 31. Mai 2009 vor (LT-Drs. 5/2943).

Die Zusammenarbeit auf der Ebene der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** und in ihren Arbeitskreisen hat stetig zugenommen. Das ist auch durch neue Arbeitskreise bedingt, wie den AK Grundsatzfragen und den AK Bildung. Auch wurde der AK Europa nach längerer Pause wieder aktiviert. Alle diese genannten Arbeitskreise nimmt der Landesbeauftragte weitgehend selbst wahr, im Übrigen nehmen die Bediensteten der Geschäftsstelle aus den jeweils zuständigen Referaten die Termine wahr und führen den laufenden Schriftverkehr und Erfahrungsaustausch; dies betrifft die ständigen Arbeitskreise Sicherheit, Justiz, Gesundheit und Soziales, Technik, Medien, Grundsatzfragen der Verwaltungsmodernisierung, Statistik, Personalwesen, Steuerverwaltung, Verkehr und Wissenschaft.

Im Anlagenteil dieses Berichts sind die Entschließungen der Konferenz im Berichtszeitraum aufgeführt, dazu auch einige wesentliche Beschlüsse des Düsseldorfer Kreises als der Gemeinschaft der Aufsichtsbehörden im nicht-öffentlichen Bereich. Zudem wurden Entschließungen der Europäischen Konferenz der Datenschutzbeauftragten und der Internationalen Konferenz mit aufgenommen (vgl. Kapitel 7).

2.4 Tag der offenen Tür in der Landtagsverwaltung

Am 2. und 3. Oktober 2010 veranstalteten Landesregierung und Landtag anlässlich des 20-jährigen Bestehens des Landes Sachsen-Anhalt einen Tag der offenen Tür.

Der Landesbeauftragte für den Datenschutz beteiligte sich an beiden Veranstaltungstagen und hatte im Landtagsgebäude einen eigenen Stand aufgebaut, um seine Arbeit vorzustellen. Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle und der Landesbeauftragte selbst standen für Gespräche mit Bürgerinnen und Bürger zur Verfügung. Hierfür hatte der Landesbeauftragte Materialien zum Datenschutz und zur Informationsfreiheit bereitgestellt, die bereits am ersten Tag einen regen Zuspruch fanden.

Insbesondere Themen wie Arbeitnehmerdatenschutz, Videoüberwachung, Volkszählung und Datenschutz im Internet wurden in der zweitägigen Veranstaltung von Interessierten angefragt und mit dem Landesbeauftragten für den Datenschutz und seinem Team diskutiert.

Der Landesbeauftragte wird auch künftig ähnliche Veranstaltungen nutzen, um den Bürgerinnen und Bürgern den Datenschutz und die Informationsfreiheit in ihrer Vielfalt näher zu bringen.

2.5 Informationszugangsgesetz Sachsen-Anhalt

Im IX. Tätigkeitsbericht hatte der Landesbeauftragte unter Nr. 2.4 über das Inkrafttreten des Informationszugangsgesetzes Sachsen-Anhalt (IZG LSA) zum 1. Oktober 2008 und seine neue Aufgabe als Landesbeauftragter für die Informationsfreiheit berichtet.

Am 14. Dezember 2010 hat der Landesbeauftragte der Öffentlichkeit seinen ersten Tätigkeitsbericht zur Informationsfreiheit vorgestellt. Der Text entspricht der LT-Drs. 5/3001 und umfasst den Zeitraum von dem Inkrafttreten des Gesetzes am 1. Oktober 2008 bis zum 30. September 2010. Zwei Jahre nach Inkrafttreten des IZG LSA konnte der Landesbeauftragte dabei eine erste erfolgreiche Bilanz ziehen. Das junge Gesetz, das jedermann einen voraussetzungslosen Anspruch auf Zugang zu amtlichen Informationen gewährt, hat sich grundsätzlich bewährt. Die Verwaltung wird transparenter. Infolge der gesetzlich geregelten Ausschlussgründe, bei denen ein Informationszugang zum Schutz öffentlicher oder privater Belange versagt werden kann, wird sie jedoch niemals gläsern sein. In seinem Tätigkeitsbericht ist der Landesbeauftragte insbesondere auf Sachverhalte eingegangen, in denen das Spannungsverhältnis der Informationsfreiheit zum Datenschutz relevant wurde (vgl. Nrn. 3.8.3, 5.1, 5.4, 5.5, 5.6, 5.11 und 5.15 des I. Tätigkeitsberichts zur Informationsfreiheit). Die Regelungen zum Schutz personenbezogener Daten sind in Sachsen-Anhalt dabei so strikt, dass personenbezogene Daten nach dem IZG LSA regelmäßig vor purer Neugier oder Sensationslust eines Antragstellers geschützt bleiben. Im Übrigen hat der EuGH in seinem Urteil vom 9. November 2010 zur Veröffentlichung der Empfänger von Agrarsubventionen (EuGH, Rechtssache C-92/09 und C-93/09; NJW 2011, 1338) gezeigt, dass das Spannungsverhältnis zwischen Informationsfreiheit und Datenschutz so aufgelöst werden kann, dass beiden Seiten hinreichend Rechnung getragen wird (vgl. Nr. 3.8.3 des I. Tätigkeitsberichts zur Informationsfreiheit).

Nach § 12 Abs. 3 IZG LSA i. V. m. § 22 Abs. 4a Satz 2 DSG-LSA hat die Landesregierung zum Bericht Stellung genommen (LT-Drs. 6/131). Der Landtag von Sachsen-Anhalt hat beschlossen, sich mit dem ersten Tätig-

keitsbericht zur Informationsfreiheit zu befassen und diesen öffentlich zu debattieren (LT-Drs. 5/88/3072 B).

Die Landesregierung hat auch in einer Antwort auf eine Kleine Anfrage zum IZG LSA die Aufnahme des IZG LSA in das Landesrecht als erfolgreich bewertet. Als Erfolg des Gesetzes sei die mit ihm vollzogene Prioritätenumkehr, nämlich die generelle Abkehr vom Aktengeheimnis zur Aktenöffentlichkeit, zu sehen (LT-Drs. 5/3146, zu 6.).

3 Allgemeines Datenschutzrecht

3.1 Novellierung des Datenschutzrechts

Schon im VIII. Tätigkeitsbericht (Nr. 3.1) und im IX. Tätigkeitsbericht (Nr. 3.1) hat der Landesbeauftragte die Notwendigkeit der Anpassung von Datenschutzgesetzen und -regelungen an die sich schnell verändernden Verhältnisse angesprochen. Meinungen und Forderungen wurden dargestellt und erste gesetzgeberische Vorhaben in Teilbereichen des Datenschutzrechts beschrieben. Im Koalitionsvertrag zwischen CDU, CSU und FDP für die 17. Legislaturperiode wird ein moderner Datenschutz als von besonderer Bedeutung in der heutigen Informationsgesellschaft angesehen. Ein hohes Datenschutzniveau sei gewollt. Unter anderem war die Absicht formuliert, das BDSG unter Berücksichtigung der europäischen Rechtsentwicklung verständlicher und zukunftsfest zu machen. Im Dezember 2010 fasste der Bundestag eine Entschließung (BT-Drs. 17/4179), in der u. a. die große Bedeutung eines präventiven technologischen Datenschutzes unterstrichen wird, eine Stärkung der Betroffenenrechte und weitere Regelungen gefordert werden, die den Gefahren für die Persönlichkeitsrechte durch den Einsatz moderner Technologien begegnen (s. auch oben Nr. 1.2).

Auch die Datenschutzbeauftragten des Bundes und der Länder sehen weiter dringenden Handlungsbedarf. Die Entwicklungen des Internets führen zu immer mehr und unüberschaubareren Datenverarbeitungen. Preiswerte Überwachungstechniken und mobile Medien, wie z. B. Smartphones mit ihren vielfältigen Nutzungsmöglichkeiten, erleichtern die Überwachung und ausufernde Verknüpfung von Daten. Dies führt zu Gefährdungen des Persönlichkeitsrechts des Einzelnen, der seinen Datenschatten nicht mehr überblicken und erst recht nicht mehr steuern kann. Es stellen sich zunehmend die Fragen, wie der Einzelne geschützt wird gegenüber nicht gewollten Persönlichkeitsprofilen und Ausforschung seiner Person über das Internet und neue Medien. Die Datenschutzgesetze aus dem Zeitalter vor dem Internet bieten keine ausreichenden Antworten. Ein novelliertes Datenschutzrecht muss sich daher den neuen Technologien anpassen und die Rechte der Betroffenen klar definieren und ihre Ausübung gewährleisten. Neben den rechtlichen Vorgaben ist es allerdings auch notwendig, Datenschutz in Staat, Wirtschaft und Gesellschaft zu praktizieren. Es muss eine Datenschutzkultur gelebt werden, deren Inhalt auch transportiert wird. Datenschutz ist daher auch als Bildungsaufgabe zu verstehen, insbesondere, um der jungen Generation den verantwortungsvollen Umgang mit eigenen und den respektvollen Umgang mit fremden Daten nahe zu bringen. Zu diesen Aspekten erging die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und

der Länder im Oktober 2009 „Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur“ (**Anlage 1**).

Die bisherigen Defizite im legislativen Bereich haben die Datenschutzbeauftragten des Bundes und der Länder veranlasst, sich an der Diskussion über Novellierungsbedarf und -möglichkeiten aktiv zu beteiligen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb Eckpunkte formuliert, die Grundlage der Diskussion über eine Reform des Datenschutzrechts sein sollen. Hierzu entstand das **Eckpunktepapier** „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ (das Eckpunktepapier ist auf der Homepage veröffentlicht, zur Zusammenfassung s. **Anlage 7**). Danach sollten in novellierten Datenschutzgesetzen konkrete Schutzziele und Grundsätze verankert werden. Technikneutrale Vorgaben sollten den Gefährdungen der technischen Entwicklung entgegenwirken, und das Datenschutzrecht sollte internetfähig gemacht werden. Die Betroffenenrechte müssen gestärkt werden. Notwendig sind weiter die Verbindlichkeit der Eigenkontrolle der verantwortlichen Stellen, die Stärkung der Datenschutzaufsicht und wirksame Sanktionen.

Auch auf europäischer Ebene schreitet die Entwicklung des Datenschutzrechts voran. Mit dem Vertrag von Lissabon, der seit dem 1. Dezember 2009 in Kraft ist, wird nicht nur die Beteiligung des Europäischen Parlaments beim Erlass datenschutzrelevanter Regelungen gestärkt. Bestandteil des Vertrages ist auch die Charta der Grundrechte der Europäischen Union. Damit sind die Artikel 7 (u. a. Achtung des Privat- und Familienlebens) und Artikel 8 (Schutz der personenbezogenen Daten) bei der Umsetzung von EU-Recht rechtlich bindend.

Darüber hinaus hat die Europäische Kommission im Herbst 2010 ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ formuliert (KOM(2010) 609 endgültig). Darin wird festgestellt, dass die europäische Datenschutzrichtlinie aus dem Jahr 1995 (Richtlinie 95/46/EG) zwar ein Meilenstein in der Entwicklung der Datenschutzpolitik der Europäischen Union war. Infolge der technologischen Entwicklung stelle sich aber die Frage, ob die Datenschutzbedingungen der Europäischen Union den aktuellen Herausforderungen Stand halten. Daher werde ein Konzept mit dem Ziel vorgelegt, die lückenlose Einhaltung des Grundrechts des Einzelnen auf Schutz seiner Daten zu garantieren. Auch dieses Konzept sieht u. a. eine Stärkung der Rechte des Einzelnen, mehr Transparenz, eine Förderung des Datenschutzbewusstseins und eine höhere Verantwortung der Datenverarbeiter vor. Die Datenschutzbeauftragten des Bundes und der Länder befürworteten die Vorstellungen der Kommission. Ergänzend wurde u. a. angeregt, dem Rechtsschutz im Internet und dem Schutz vor Profilbildung mehr Beachtung zu schenken.

Die Kommission wertet die Ergebnisse des Konsultationsprozesses aus und will noch im Jahre 2011 Vorschläge für eine kohärente Neuregelung, d. h. nicht nur den Binnenmarkt, sondern auch die Bereiche Sicherheit und Justiz erfassend, vorlegen (möglicherweise teilweise auch in Form einer Verordnung). Das Europäische Parlament unterstützt die Vorstellungen und betont auch eine Stärkung der Datenschutzbehörden.

3.1.1 BDSG-Novellen 2009 – Novellierung des Landesrechts?

Zu Gesetzesvorhaben als politische Konsequenz aus den Datenskandalen aus dem Jahr 2008 hatte der Landesbeauftragte im IX. Tätigkeitsbericht (Nr. 3.1) informiert. Die Kritik von Datenschutzbeauftragten und Verbraucherschützern hat letztlich dazu geführt, dass zum Ende der 16. Legislaturperiode Novellen des BDSG erlassen wurden.
In einer Novelle zum BDSG (BT-Drs. 16/10529) standen intransparente Verfahrensweisen der Auskunfteien insbesondere beim Einsatz sogenannter Scoringverfahren und nicht nachvollziehbare Entscheidungen von Geschäftspartnern im Vordergrund. Es wurden die Rechte der Betroffenen durch Informations- und Auskunftsrechte gestärkt. Die Änderungen traten am 1. April 2010 in Kraft (BGBl. 2009 I S. 2254).

Eine weitere BDSG-Novelle (BT-Drs. 16/13657) entstand in Reaktion auf die Datenschutzskandale, die den illegalen Datenhandel (Adresshandel) und die Verwendung von Beschäftigtendaten zu deren Ausforschung betrafen. Zunächst bestand im Interesse der Betroffenen die politische Absicht, dass die Verwendung von personenbezogenen Daten zu Zwecken der Werbung, Markt- und Meinungsforschung künftig grundsätzlich nur noch mit ausdrücklicher Einwilligung der Betroffenen zulässig sein sollte. Zudem sollten marktbeherrschende Unternehmen die Einwilligung nicht durch Kopplung mit dem Vertragsschluss erzwingen dürfen. Es ist wohl auf massive Lobbyarbeit zurückzuführen, dass die Verwendung listenmäßig oder sonst zusammengefasster Daten zum Zwecke der Werbung ohne Einwilligung der Betroffenen letztlich u. a. doch zulässig ist, wenn bestimmte Transparenzaspekte beachtet werden (§ 28 Abs. 3 Satz 4 BDSG). In § 32 BDSG wurde die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses in einem Paragraphen pauschal geregelt (vgl. Nr. 3.1.2). Das Erforderlichkeitskriterium wurde betont. Die Verwendung von Daten für die Aufdeckung von Straftaten, also repressives Vorgehen, wurde an tatsächliche Anhaltspunkte für den Verdacht geknüpft, der Beschäftigte habe eine Straftat begangen. Zudem wurden die Regeln auch auf nicht automatisierte Verarbeitung erstreckt. Weiter wurden u. a. die Stellung der betrieblichen Datenschutzbeauftragten gestärkt (§ 4f Abs. 3 Satz 5 bis 7 BSDG) und die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten eingeführt (§ 42a BDSG). Die Regelungen traten weitestgehend am 1. September 2009 in Kraft (BGBl. I S. 2814).

Für den Bereich des Landesdatenschutzgesetzes hat sich aus diesen Entwicklungen weiterer Novellierungsbedarf ergeben:

- Stärkung der Stellung des behördlichen Datenschutzbeauftragten
- Informationspflicht bei Datenpannen
- Verschärfung der Regelung zur Auftragsdatenverarbeitung
- und daneben: Neuregelung für gemeinsame automatisierte Verfahren mehrerer Stellen.

Das Ministerium des Innern zögert noch mit einer Gesetzesinitiative, auch wenn der Bedarf schon seit 2009 nicht verkannt wird. Andere Länder sind bereits weiter. Der vom Ministerium betonte Aspekt einer Rechtsvereinheitlichung sollte nicht vorgeschoben werden; denn die grundlegende Novellierung des Datenschutzrechts auf nationaler und europäischer Ebene (Nr. 3.1) wird nicht in ein paar wenigen Jahren erfolgt sein.

3.1.2 Arbeitnehmerdatenschutz

Auch die Verbesserung des Arbeitnehmerdatenschutzes ist erklärtes Ziel in der Koalitionsvereinbarung auf Bundesebene. Mitarbeiter sollten wirksam vor Bespitzelungen geschützt werden. Arbeitgeber sollten verlässliche Regelungen für den Kampf gegen Korruption an die Hand bekommen. Auch die Datenschutzbeauftragten des Bundes und der Länder hatten seit sehr langer Zeit differenzierte Neuregelungen zum Datenschutz im Beschäftigungsverhältnis gefordert (vgl. Nr. 3.1 im IX. Tätigkeitsbericht).
Nunmehr liegt ein Gesetzentwurf der Bundesregierung (BT-Drs. 17/4230) neben Entwürfen der Bundestagsfraktionen der SPD und von BÜNDNIS 90 / DIE GRÜNEN vor, der eine differenzierte Neuregelung in den §§ 32 bis 32l BDSG enthält. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits frühzeitig Gelegenheit, sich zu dem zugrunde liegenden Entwurf des Bundesministers des Innern zu äußern. In der Entschließung der Konferenz vom 22. Juni 2010 „Beschäftigtendatenschutz stärken statt abbauen“ (**Anlage 13**) wurde auf einige kritische Punkte hingewiesen. Auch der Stellungnahme des Bundesrates zu dem Entwurf lassen sich viele differenzierte und auch kritische Anmerkungen entnehmen (BR-Drs. 535/10).
Zunächst ist zwar zu begrüßen, dass nun endlich eine ausdifferenzierte Regelung erfolgen soll. So soll beispielsweise die heimliche Videoüberwachung verboten werden, es wird der Zugriff des Arbeitgebers auf Internetinformationen zu Bewerbern reglementiert und eine Compliance-Regelung getroffen. Das eigentliche Ziel, den Beschäftigten vor übermäßiger Überwachung und Kontrolle zu schützen, wird aber in wesentlichen Punkten verfehlt. Dabei ergab sich der Handlungsdruck zur Schaffung einer Neuregelung gerade aus den Skandalen des Jahres 2008, die einen angemessenen Ausgleich zwischen legitimen Arbeitgeberinteressen und dem Schutz des Persönlichkeitsrechts des Beschäftigten nötig machten.
Beispielhaft sei darauf verwiesen, dass nunmehr erhebliche Ermittlungsbefugnisse des Arbeitgebers zur Verhinderung und Aufdeckung von Vertragsverletzungen vorgesehen sind, die Einschränkung der Internetnutzung im Bewerbungsverfahren zu schwach ist oder sog. „Whistleblower“ nicht hinreichend geschützt werden, obwohl gerade die internen Informationsgeber zur Aufdeckung der Skandale im Jahr 2008 führten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die wesentlichen datenschutzrechtlichen Anliegen für die Diskussion der Entwürfe in der Entschließung vom März 2011 „Beschäftigtendatenschutz stärken statt abbauen“ zusammengefasst (**Anlage 19**). In einer Anhörung im Bundestagsinnenausschuss am 23. Mai 2011 prallten Arbeitgeber- und Arbeitnehmerpositionen aufeinander.

Die Regelungen der §§ 32 ff. BDSG fänden allerdings infolge der Subsidiarität des BDSG auf Beschäftigte der unmittelbaren oder mittelbaren Landesverwaltung keine Anwendung. Sie dürften sich aber auf die Rechtsprechung

auswirken. Auch sollten die Länder nach Auffassung des Bundesrates prüfen, ob eine Rechtseinheitlichkeit herzustellen ist.

3.1.3 Regulierung georeferenzierter Daten im Internet

Befördert durch die von allen politischen und gesellschaftlichen Schichten geführte Diskussion um Google Street View und seine Möglichkeit, 360°-Panoramabilder aus der Straßenperspektive darzustellen, hatte im Juli 2010 der Bundesrat einen Gesetzesantrag zur Änderung des Bundesdatenschutzgesetzes (BDSG) beschlossen. Dieser auf eine Initiative der Freien und Hansestadt Hamburg zurückgehende Gesetzesantrag regt an, durch einen neuen § 30b im BDSG quasi eine lex Google Street View zu schaffen. Unter dem sperrigen Namen „Geschäftsmäßige Datenerhebung und -speicherung im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Geodaten zum Zweck des Bereithaltens fotografischer oder filmischer Panoramaaufnahmen im Internet zum Abruf für jedermann oder zur Übermittlung an jedermann“ (BT-Drs. 17/2765) sollen die Rahmenbedingungen für die Zulässigkeit der Erhebung und weiteren Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Gebäuden und Straßen zum Zweck des Bereithaltens von Panoramaaufnahmen im Internet zum Abruf für jedermann erhoben werden, festgelegt werden. Neben der Schaffung einer allgemeinen Befugnisnorm für die Erhebung personenbezogener Daten im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Gebäuden und Straßen zum Zweck des Bereithaltens fotografischer oder filmischer Panoramaaufnahmen im Internet zum Abruf für jedermann soll für die verantwortliche Stelle eine gesetzliche Verpflichtung begründet werden, Personen und amtliche Kennzeichen von Fahrzeugen vor ihrer Übermittlung unkenntlich zu machen. Des Weiteren soll Eigentümern, Mietern, Fahrzeughaltern und sonstigen Betroffenen das Recht eingeräumt werden, der weiteren Verarbeitung und Nutzung ihrer personenbezogenen Daten widersprechen zu können, die derart georeferenziert zum Abruf bereitgestellt werden sollen. Im Fall des Widerspruchs gegen die weitere Verarbeitung und Nutzung sind die personenbezogenen Daten nach dem Gesetzentwurf zu anonymisieren oder zu löschen.

Aufgrund der anhaltenden öffentlichen Diskussion hat die Politik reagiert. So stellte das Bundesministerium des Innern im Juni 2010 seine „Thesen zur Netzpolitik“ vor, die grundlegende Werte, maßvolle und ausgleichende Rechtsentwicklung und Eigenverantwortung und Selbstkontrolle betonen. Bundesinnenminister Friedrich folgt hierzu im Übrigen den Positionen seines Amtsvorgängers de Maizière. Im September 2010 fand ein Spitzengespräch beim Bundesministerium des Innern statt. Zu diesem Spitzengespräch unter dem Oberbegriff „Digitalisierung von Stadt und Land“ waren neben einer ganzen Reihe von Vertretern der Geoinformationswirtschaft (GIW) und der Politik auch einige wenige Beauftragte für den Datenschutz eingeladen. Ziel des Gespräches sollte es sein, den Handlungsbedarf für Wirtschaft und Verwaltung im Bereich des Umganges mit georeferenzierten Daten einer umfassenden Betrachtung zu unterziehen und Lösungsmöglichkeiten auszuloten. Außerdem sollte das Gespräch Auftakt zu einer Diskussion über die Modernisierung und Anpassung des Datenschutzrechts im Internetzeitalter sein. Die Ausweitung der Befassung mit dem Umgang mit georeferenzierten Daten über das im Fokus der Öffentlichkeit stehende Street View hinaus war zwin-

gend geboten. Die private Wirtschaft, aber auch die öffentliche Verwaltung erheben, verarbeiten und nutzen in immer größerem Umfang georeferenzierte Daten. Auch die massenhafte Verbreitung von Smartphones hat die Nutzung von Lokalisierungsdiensten zu einem wachsenden Problem werden lassen. Die Gefahr unerwünschter bzw. unbemerkter persönlichkeitsbeeinträchtigender Profilbildung nimmt damit neue Dimensionen an.

Das Bundesministerium des Innern betonte in der Folge den notwendigen Schutz der informationellen Selbstbestimmung gegenüber Unternehmen und dem Staat. Betont wurden aber auch die Werte der Freiheit und Eigenverantwortung. Der Einzelne habe auch das Recht, Informationen über sich und andere zu verarbeiten und ggf. Dummheiten zu begehen. Auch seien die Interessen einer starken und innovativen IT-Wirtschaft zu beachten.

Ein Interessenausgleich sei nötig. Ziel des Bundesministeriums des Innern sei es, Grenzen vorzugeben, jenseits eines Kernbereiches des Persönlichkeitsschutzes auch Freiheiten zur Selbstregulierung zu wahren. Dies führte u. a. zu zwei Ergebnissen:

a. Datenschutz-Kodex zu Google Street View und ähnlichen Diensten

   Die GIW sollte bis zum Dezember 2010 einen Datenschutz-Kodex für Geodatendienste vorlegen. Ziel dieses Kodex sollte sein, die Akzeptanz der neuartigen Geodatendienste und die informationelle Selbstbestimmung der Nutzer zu fördern. Der Kodex soll im Wege der Selbstverpflichtung der GIW Grundsätze für einen angemessenen Ausgleich der Interessen von Betroffenen, Nutzern und Anbietern der Dienste festlegen.
   Der Entwurf eines solchen Kodex wurde vorgelegt. Hielt man sich vor Augen, aus wessen Feder er stammte, überraschte nicht, dass er noch erhebliche datenschutzrechtliche Defizite manifestierte. Durch den Düsseldorfer Kreis wurden dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) die bedenklichen Regelungsinhalte aufgezeigt und Änderungsvorschläge unterbreitet, die vor allem auf einen Vorabwiderspruch vor der Veröffentlichung zielten. Im Rahmen seiner Mitarbeit in der Unterarbeitsgruppe Geodaten des Arbeitskreises Grundsatzfragen der Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich auch der Landesbeauftragte in die Diskussion eingebracht.
   Der Kodex wurde am 1. März 2011 durch die BITKOM an das Bundesministerium des Innern übergeben. Verbindlich wird er jedoch erst, wenn die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) ihm zustimmen, was jedoch wegen der verbliebenen erheblichen datenschutzrechtlichen Bedenken fraglich ist. Der Düsseldorfer Kreis hat in einem Beschluss vom 8. April 2011 (**Anlage 28**) diese datenschutzrechtlichen Bedenken veröffentlicht und stellte darin fest, dass nunmehr der Gesetzgeber gefordert sei.

b. Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Das Bundesministerium des Innern stellte – nachdem sich die Innenministerkonferenz für den Entwurf des Bundesrates eingesetzt hatte – im Dezember 2010 den Entwurf eines Gesetzes zur Änderung des BDSG zur Diskussion. Unter dem Namen „Unzulässige Veröffentlichungen in Telemedien“, in Presse und Öffentlichkeit besser als **Rote-Linie-Gesetz** bekannt, soll ein neuer § 38b eingeführt werden. Dieser Entwurf sieht u. a. vor, die Veröffentlichung personenbezogener Daten in Telemedien (also dem Internet) dann für unzulässig zu erklären, wenn ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen herbeigeführt würde. Dass im Umkehrschluss alle durch Telemedienveröffentlichungen verursachten minderschweren Persönlichkeitsrechtseingriffe möglicherweise legitimiert würden, war nur einer der Kritikpunkte. Der Gesetzentwurf, der weit über die Verarbeitung von Geodaten hinausgeht, z. B. auch sog. Profilbildungen problematisiert, wird noch über das Ende des Berichtszeitraumes hinaus kontrovers diskutiert. Eine ausschließliche Selbstregulierung im Bereich der virtuellen Welt würde den Schutz der Privatsphäre verkürzen.

3.1.4 Stiftung Datenschutz

Der Koalitionsvertrag auf Bundesebene sieht für den Datenschutz unter anderem vor, eine Stiftung Datenschutz zu errichten. Sie soll den Auftrag haben, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, ein Datenschutzaudit zu entwickeln, Bildung im Bereich des Datenschutzes zu stärken und den Selbstdatenschutz durch Aufklärung zu verbessern. Auch an die Forschung und die Weiterentwicklung des Datenschutzes wird gedacht.

Die sachdienliche Besetzung der Organe der Stiftung und ihre Ausstattung werden diskutiert. Wichtig erscheint dabei die Unabhängigkeit der Stiftung von Geldgebern. Insbesondere ist das Verhältnis zur Datenschutzaufsicht durch die Beauftragten klar abzugrenzen. Bei der Ausgestaltung der ergänzenden Funktionen der Stiftung haben die Datenschutzbeauftragten des Bundes und der Länder ihre Mitwirkung angeboten. Sie fassten hierzu auf der 80. Konferenz im November 2010 die Entschließung „Förderung des Datenschutzes durch Bundesstiftung“ (**Anlage 16**). Die Vorbehalte sind nicht ausgeräumt, das Vorhaben ruht.

3.2 Effektive und unabhängige Datenschutzaufsicht

Im VIII. Tätigkeitsbericht (Nr. 3.3) und im IX. Tätigkeitsbericht (Nr. 3.2) hatte der Landesbeauftragte ausführlich zur Frage der Unabhängigkeit der Datenschutzaufsicht berichtet. Insbesondere wurde auf das Vertragsverletzungsverfahren der Kommission der Europäischen Gemeinschaften hingewiesen.
Im Vertragsverletzungsverfahren erging die Entscheidung des Europäischen Gerichtshofs am 9. März 2010 (C- 518/07, NJW 2010, 1265). Dieser stellte fest, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG verstoßen hat, indem die

zuständigen Kontrollstellen in den Bundesländern für die Überwachung der Verarbeitung von personenbezogenen Daten durch nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen staatlicher Aufsicht unterstellt sind. Das Erfordernis „völliger Unabhängigkeit“ sei damit falsch umgesetzt.
Der Forderung auch der Datenschutzbeauftragten (vgl. VIII. Tätigkeitsbericht, Nr. 3.3) nach Unabhängigkeit wurde bisher in Deutschland teilweise entgegen gehalten, es sei nur funktionelle Unabhängigkeit geboten. Das Demokratieprinzip fordere die parlamentarische Verantwortung der Regierung und die Weisungsgebundenheit der Verwaltung. Die Tätigkeit einer Aufsichtsbehörde, die Verwaltungsakte im nicht-öffentlichen Bereich erlasse, dürfe kein ministerialfreier Raum sein.
Hierzu stellt der EuGH fest, dass das Demokratieprinzip zur Gemeinschaftsrechtsordnung gehöre. Das bedeute aber nicht, dass es außerhalb des klassischen Verwaltungsaufbaus keine Stellen geben könne, die von der Regierung mehr oder weniger unabhängig sind. Das Bestehen und die Bedingungen solcher Stellen sind in den Mitgliedsstaaten durch Gesetz oder sogar die Verfassung geregelt, die Stellen unterliegen dem Gesetz und der gerichtlichen Kontrolle. Diese Stellen hätten häufig Regulierungsfunktion oder nähmen Aufgaben wahr, die der politischen Einflussnahme entzogen sein sollen. Demnach ist davon auszugehen, dass eine Ausgestaltung der Aufsichtsbehörde in Fachaufsicht, aber auch in Rechtsaufsicht europarechtlich nicht zulässig wäre. Fraglich ist nur, ob eine Dienstaufsicht ohne Verstoß gegen das Unabhängigkeitsgebot vorgesehen werden kann. Im Hinblick auf die vorgenannten strengen Vorgaben dürfte die Dienstaufsicht dabei wohl lediglich als die Aufsicht über das persönliche Verhalten des Betroffenen anzusehen sein. Möglich erscheint eine Anlehnung an das auch vom EuGH nicht kritisierte Richterrecht, wonach eine Dienstaufsicht gegeben ist, soweit nicht die Unabhängigkeit beeinträchtigt wird.

Sachsen-Anhalt ist von der Entscheidung des EuGH betroffen, da neben dem Landesbeauftragten das Landesverwaltungsamt für den Datenschutz im nicht-öffentlichen Bereich zuständig ist. Der Landesbeauftragte forderte daraufhin erneut eine sofortige Bündelung der Datenschutzaufsicht über den privaten und den öffentlichen Bereich in seiner Behörde.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Entschließung der 79. Konferenz vom 17./18. März 2010 „Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle“ (**Anlage 8**) die Gesetzgeber aufgefordert, schnellstmöglich die Vorgaben der Richtlinie umzusetzen und die im einzelnen aufgeführten Kriterien der Unabhängigkeit zu berücksichtigen.

Ein Entwurf der Fraktion der FDP zur Änderung des DSG-LSA (LT-Drs. 5/2487) vom Frühjahr 2010 sah die Zusammenführung der Datenschutzaufsicht im öffentlichen sowie im nicht-öffentlichen Bereich beim Landesbeauftragten für den Datenschutz vor.

Im Rahmen der Anhörung des Ausschusses für Inneres des Landtags von Sachsen-Anhalt wurden einige externe Landesdatenschutzbeauftragte beteiligt. Die Stellungnahmen bewerteten die rechtliche Gleichstellung mit einer obersten Landesbehörde positiv und sprachen sich für die Zusammenlegung

des öffentlichen und nicht-öffentlichen Bereichs aus.
Der Landesbeauftragte hatte vor dem Ausschuss Gelegenheit, die Anforderungen an die Unabhängigkeit näher darzulegen. Neben anderen Aspekten spricht der Aspekt eines effektiven Grundrechtsschutzes für die Zusammenlegung der Aufsicht beim Landesbeauftragten. Die Unabhängigkeit ist gewahrt, wenn die Stellung einer obersten Landesbehörde vorgegeben ist. Zudem wurde auf die gebotene Mehrausstattung mit personellen und Sachmitteln hingewiesen.

Der Gesetzentwurf wurde dann allerdings im November 2010 von der Tagesordnung abgesetzt und verfiel letztlich in der 5. Legislaturperiode der Diskontinuität. Dem lag u. a. die vom Innenministerium geförderte Überlegung zugrunde, dass zunächst eine Zusammenführung der Datenschutzaufsicht der Länder Sachsen, Thüringen und Sachsen-Anhalt geprüft werden solle. Dies blieb jedoch stecken. Gegen eine solche Mitteldeutschlandvariante sprechen erhebliche rechtliche und tatsächliche Gründe; so wäre auch die Erarbeitung eines Staatsvertrages notwendig.

Die Landesregierung hielt an ihrer Skepsis gegenüber dem EuGH-Urteil fest und unterstützte infolge auch eines Votums der Innenministerkonferenz noch in der Bundesratssitzung am 11. Februar 2011 im Rahmen der Stellungnahme zum Gesamtkonzept der Europäischen Kommission für den Datenschutz in der Union (s. Nr. 3.1) einen Antrag, wegen angeblicher Demokratiedefizite bei einer Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich im Falle völliger Unabhängigkeit die Europäische Datenschutzrichtlinie dergestalt zu ändern, dass die Aufsichtsbehörden nur von den zu kontrollierenden Stellen unabhängig sein müssen (BR-Drs. 707/1/10, Nr. 15). Die Beachtung der Richtlinie sollte mittels deren Änderung erfolgen bzw. die europarechtswidrige Nichtbeachtung so umgangen werden. Der Landesbeauftragte war über diese Position befremdet und hätte hierzu eine vorherige Beteiligung für sinnvoll erachtet. Der Bundesrat folgte dem Antrag im Ergebnis mehrheitlich nicht (BR-Drs. 707/10 (Beschluss)).

Auch wenn sich das Innenministerium nach dem Urteil des EuGH weitgehend der konkreten Fach- und Rechtsaufsicht über das Landesverwaltungsamt enthielt, war der Handlungsdruck unverändert gegeben (vgl. auch Beschluss des Landtages vom 3. Februar 2011, LT-Drs. 5/88/3072 B). Die Europäische Kommission mahnte im April 2011 eine europarechtskonforme Regelung an.

Mit dem Gesetzentwurf der Koalitionsfraktionen – auf der Grundlage von Vorarbeiten des Innenministeriums – in LT-Drs. 6/86 vom 1. Juni 2011 sollen die europäischen Vorgaben nun umgesetzt werden. Auch hier klingen noch Restzweifel an der demokratisch und rechtsstaatlich verankerten Position eines unabhängigen Datenschutzbeauftragten an. Der Landesbeauftragte warb in einer Anhörung vor dem Innen- und dem Rechtsausschuss des Landtages im August 2011 für eine kohärente Regelung und zugleich zwecks Wahrung der materiellen Unabhängigkeit für die notwendige erhebliche Mehrausstattung. Im Übrigen schlug der Landesbeauftragte vor, entsprechend Vorbildern in anderen Ländern eine mit Landtagsabgeordneten besetzte Datenschutzkommission einzurichten, die den Landesbeauftragten in seiner Tätigkeit unterstützen und auch so den Stellenwert des Datenschutzes

im Land Sachsen-Anhalt stärken könne. Dazu kam es nicht. Die zusätzliche Aufgabe der Aufsicht über den nicht-öffentlichen Bereich obliegt dem Landesbeauftragten ab 1. Oktober 2011 (LT-Drs. 6/321).

Der XI. Tätigkeitsbericht wird näher auf Entwicklungen des Datenschutzes im nicht-öffentlichen Bereich eingehen.

3.3 Europäischer Datenschutztag

Der Europarat hat den 28. Januar als jährlich zu begehenden Datenschutztag ausgerufen, um das Bewusstsein für den Datenschutz in Europa zu stärken (s. Nr. 3.3 des IX. Tätigkeitsberichts).
Am 28. Januar 2011 fand anlässlich des Fünften wie auch anlässlich früherer Europäischer Datenschutztage eine zentrale Veranstaltung der Datenschutzbeauftragten des Bundes und der Länder in Berlin statt.
Die Veranstaltung sollte dazu beitragen, die Wege und Möglichkeiten einer Gestaltung des Datenschutzrechts auf nationaler und internationaler Ebene zu eruieren, die einer modernen Informationsgesellschaft und insbesondere den technischen Gefahren für das Persönlichkeitsrecht des Einzelnen gerecht wird. Hochrangige Vertreter der Bundesregierung, Vertreter der europäischen Ebene (Parlament und Kommission), der Wissenschaft und der Wirtschaft konnten ihre Vorstellungen in Vorträgen und in einer Podiumsdiskussion darstellen. Auch die Datenschutzbeauftragten hatten Gelegenheit, den von ihnen erkannten Veränderungsbedarf anzusprechen und das von ihnen entworfene Eckpunktepapier zur Modernisierung des Datenschutzes in den Blick der Öffentlichkeit zu stellen (s. Nr. 3.1).

Die Vertreter der europäischen Ebene konnten auf die neue Rechtslage durch den Vertrag von Lissabon hinweisen.
Vertreter der Wissenschaft strukturierten den Optimierungsbedarf in drei Ebenen. Zunächst gehe es um die klassischen Bereiche staatlicher bzw. privater Datenverarbeitung. Als zweites sei das Web 2.0 und seine Verknüpfungen zu betrachten. Künftig komme auch das „Internet der Dinge“ hinzu. Hierzu wurden Regelungsmethoden und technische Unterstützungsmöglichkeiten diskutiert.
Seitens der Bundesregierung wurde auf den Handlungsbedarf und Handlungswillen der deutschen und europäischen Politik verwiesen.
Insgesamt erfreute sich die Veranstaltung einer hohen Besucherzahl und eines angemessenen öffentlichen Interesses.

4 Entwicklung der automatisierten Datenverarbeitung

4.1 IT-Strategie – Landesleitlinie Informationssicherheit

Der Landesbeauftragte hat in seinem IX. Tätigkeitsbericht (Nr. 4.4) über die seit Jahren andauernden Bemühungen zur Erarbeitung einer IT-Sicherheitsstrategie für das Land berichtet.

Mit dem Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619) wurden Festlegungen getroffen, welche die Belange des Datenschutzes und der Datensicherheit berücksichtigen. Eine Landesleitlinie Informationssicherheit (LL IS) soll dem-

nach die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in den Ressorts bilden. Im damaligen Beschluss zur IT-Strategie wurde noch von „IT-Sicherheit“ gesprochen, für die Landesleitlinie soll aber die **Informationssicherheit** bei allen Verwaltungsprozessen und Fachaufgaben berücksichtigt werden. Vorgesehen war als mittelfristige Maßnahme der IT-Strategie, den Datenschutz – als Bestandteil des IT-Managements – in die LL IS zu integrieren, um damit bei der Modernisierung der Verwaltung die Beachtung des informationellen Selbstbestimmungsrechts und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen.

Der Datenschutz muss dabei als integraler Bestandteil dieses IT-Managementprozesses verstanden werden. Durch eine rechtzeitige Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes zum Aufbau oder zur Änderung automatisierter Verfahren bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Unterrichtung bei automatisierten Abrufverfahren und bei Auftragsdatenverarbeitung durch Dritte, die Durchführung einer Vorabkontrolle für bestimmte automatisierte Verfahren durch die behördlichen Beauftragten für den Datenschutz, sowie die Führung von Verfahrensverzeichnissen, so die Festlegungen im Beschluss zur IT-Strategie, soll den Belangen des Datenschutzes und der Datensicherheit im Rahmen der IT-Managementprozesse entsprochen werden.

Der Landesbeauftragte hatte Gelegenheit, zu einem 1. Entwurf der LL IS der Staatskanzlei im März 2010 Stellung zu nehmen. Seine Empfehlungen, insbesondere zur Aufnahme datenschutzspezifischer Schutzziele wie Authentizität, Revisionssicherheit und Transparenz in die LL IS, wurden berücksichtigt. Er hat sich aktiv an der weiteren Ausarbeitung, in der vom IT-Koordinierungsausschuss mit Beschluss vom 25. Oktober 2010 eingesetzten Arbeitsgruppe „Informationssicherheit“ unter Leitung der Staatskanzlei, beteiligt. Mit Fertigstellung der LL IS sollte die Beschlussfassung der Landesregierung zum Aufbau eines Informationssicherheitsmanagements im Land vorbereitet werden.

Kritisch ist anzumerken, dass es beim Entwurfsstand dieser Landesleitlinie Informationssicherheit vom Februar 2011 vorerst geblieben ist, denn eine abschließende Sitzung der Arbeitsgruppe wurde im April 2011 kurzfristig abgesagt.

Der Landesbeauftragte hofft, dass nach dem Wechsel der Zuständigkeit für die IT-Strategie von der Staatskanzlei zum Ministerium für Finanzen zu Beginn der 6. Wahlperiode, auf Grund der Regierungsneubildung, die Erarbeitung der LL IS schnell zum Abschluss gebracht werden wird.

Inwieweit die nunmehr bereits drei Jahre alte IT-Strategie des Landes Sachsen-Anhalt unter den neuen Bedingungen der Zusammenarbeit vom Bund und Ländern im Rahmen des IT-Staatsvertrages und dem Aufbau eines Verbindungsnetzes durch den Bund (s. Nr. 1.3.1) einer Überarbeitung bzw. Fortschreibung bedarf, sollte ebenfalls vom jetzt zuständigen Finanzministerium überprüft werden. Der Landesbeauftragte geht davon aus, dass er rechtzeitig unterrichtet und beteiligt wird, wenn es dabei um die Lösung datenschutzrechtlicher Probleme geht.

4.2 IT-Planungsrat – spezifische Datenschutzthemen

In Vorbereitung der aus dem IT-Staatsvertrag zur Ausführung von Artikel 91c GG resultierenden Aufgaben wurde bereits mit einem Beschluss des Arbeitskreises der E-Government-Staatssekretäre vom 7. Mai 2009 die Arbeitsgruppe „IT-Planungsrat“ (IT-PLR) damit beauftragt, Vorschläge für das zukünftige Aufgabenspektrum und den Wirkungskreis sowie die Gremienstrukturen des IT-PLR zu erarbeiten. Dabei waren vor allem die bestehenden Gremien und deren Untergremien und Einrichtungen sowie die bisher bestehenden Initiativen, Vorhaben und Projekte zu berücksichtigen. Dies betraf insbesondere die Vorgängergremien des IT-PLR:

- den Arbeitskreis der E-Government-Staatssekretäre in Bund und Ländern (Aktionsplan Deutschland-Online – DOL) und
- den Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich – KoopA ADV.

Im Ergebnis wurden vom IT-PLR entsprechende Beschlüsse zu seinem Aufgabenspektrum, der Gremienstruktur und zur Aufgabenüberführung aus den Vorgängergremien DOL und KoopA ADV gefasst.

Mehr oder minder Datenschutzrelevanz für die Länder, so auch für Sachsen-Anhalt, haben danach fast alle Themen des IT-PLR, welche im **Projekt- und Anwendungsplan 2011** des IT-PLR auf seiner 3. Sitzung am 24. September 2010 beschlossen wurden. Mit einem Großteil der nachfolgend genannten Projekte sind bzw. waren die verschiedenen ständigen Arbeitskreise der Datenschutzkonferenz befasst oder daran beteiligt.

Nach diesem Projekt- und Anwendungsplan werden die bestehenden Projekte und Themenfelder in drei Kategorien unterteilt:

Kategorie 1 – **Steuerungsprojekte** des neuen Aktionsplans Deutschland-Online. (Dieser ersetzt den bisherigen Aktionsplan der Bundeskanzlerin und der Regierungschefs der Länder in der Fassung vom 21. November 2009).

Steuerungsprojekte werden nach Zuweisung durch die Bundeskanzlerin im Ergebnis der Ministerpräsidentenkonferenz durch den IT-PLR in einem Aktionsplan festgelegt. Hierzu zählen:

- Infrastruktur (Auf-und Ausbau einer abgestimmten Netzinfrastruktur der deutschen Verwaltung: Bund/Länder/Kommunen),
- Kfz-Wesen (Ziel des Vorhabens ist es, den Registrierungsprozess von Fahrzeugen unter konsequenter Nutzung der Möglichkeiten von E-Government möglichst ohne Medienbrüche online zu ermöglichen),
- Personenstandswesen (Einführung eines elektronischen Personenstandsregisters),
- Meldewesen (Aufbau eines Bundesmelderegisters; zur Zeit ruhendes Projekt),

- Nationales Waffenregister (Einführung eines einheitlichen elektronischen Systems).

Kategorie 2 – **Koordinierungsprojekte**

Koordinierungsprojekte des IT-PLR sind die bestehenden E-Government- und IT-Projekte, die eine wesentliche Komponente zur Weiternutzung im sogenannten „föderativen E-Government“ darstellen. Die Steuerung und Finanzierung bleibt hier, im Unterschied zu den Steuerungsprojekten des IT-PLR, vollständig bei den Projektverantwortlichen des Bundes, der Länder bzw. der jeweiligen Fachministerkonferenz. Hierzu zählen:

- Geodaten (Ziel: Harmonisierung der heterogenen Geoinformationsstrukturen in Deutschland zur Nutzung durch Verwaltungen, die Wirtschaft, Bürgerinnen und Bürger),

- S.A.F.E. („Secure Access to Federated E-Justice/E-Government“ - Einheitliche Kommunikationsinfrastruktur für den elektronischen Rechtsverkehr),

- D 115 (Telefonischer Bürgerservice mit der einheitlichen Behördenrufnummer 115; seit dem 14. April 2011 im Regelbetrieb).

Kategorie 3 – **Anwendungen**

Anwendungen des IT-PLR sind E-Government- bzw. IT-Lösungen, die nach einer entsprechenden Entwicklungs- und Testphase dauerhaft zur Unterstützung von automatisierten Prozessen der öffentlichen Verwaltung in Bund und Ländern regelmäßig zum Einsatz kommen. Hierzu zählen:

- DVDV (Das Deutsche Verwaltungsdiensteverzeichnis bildet die zentrale Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung und ermöglicht eine rechtsverbindliche Kommunikation zwischen Behörden über vorhandene Fachverfahren.),

- LeiKa-plus (Der sogenannte Leistungskatalog bietet Bürgerinnen und Bürgern sowie Unternehmen in Deutschland ein einheitliches, vollständiges und umfassendes Verzeichnis der Verwaltungsleistungen über alle Verwaltungsebenen hinweg. Ziel von LeiKa-plus ist es, bis Ende 2011 möglichst viele Objekte des Leistungskatalogs mit Stammtexten zu verknüpfen.),

- Behördenfinder (Mit dem Behördenfinder Deutschland wird das Informationsangebot der öffentlichen Einrichtungen standardisiert und im Zusammenwirken mit dem Portal http://www.behoerdenfinder.de umgesetzt. Die zuständigen Geschäfts- und Koordinierungsstellen für die Anwendung Leistungskatalog und Behördenfinder sind beim Ministerium des Innern des Landes Sachsen-Anhalt eingerichtet.),

- Governikus (Governikus ermöglicht den sicheren und verbindlichen elektronischen Nachrichten- und Dokumentenaustausch via OSCI und

kommt beim Bund, den Ländern und Kommunen als Basiskomponente der Virtuellen Poststelle zum Einsatz).

Neben der Geschäftsstelle des IT-PLR als ständiges Gremium wurde auf der 4. Sitzung des IT-PLR am 3. März 2011 der Start der **Koordinierungsstelle für IT-Standards** (KoSIT) beschlossen. Die KoSIT, ebenfalls eine ständige Einrichtung, hat ihre Arbeit zum 1. April 2011 in der Freien Hansestadt Bremen aufgenommen. Sie ist aus der bisherigen OSCI-Leitstelle des Landes Bremen hervorgegangen, welche bisher im Auftrag des KoopA ADV die Entwicklung fachlicher Standards für durchgehende elektronische Prozesse im Meldewesen, in der Justiz, im Ausländerwesen sowie im Personenstandswesen koordinierte und leitete. Damit wurde eine wesentliche Aufgabe des IT-PLR nach § 1 des IT-Staatsvertrages, die Beschlussfassung über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards, dauerhaft an einer Stelle gebündelt. Zukünftig wird die KoSIT zuständig sein für:

- die Koordination der Entwicklung fachlicher Standards (XÖV),
- die Pflege und Weiterentwicklung von OSCI Transport,
- die Erarbeitung fachlicher Standards im Auftrag einiger Fachministerkonferenzen.

An dieser Stelle sei nochmals auf die Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009 zum IT-Staatsvertrag (**Anlage 2**) hingewiesen. Neben der Forderung der Beteiligung der Landesbeauftragten für den Datenschutz zur Vertretung der Interessen der Länder im Bereich Datenschutz wurde vom Landtag in seinem Beschluss vom 18. März 2010 (Drucksache 5/73/2508 B) die Landesregierung aufgefordert sich dafür einzusetzen, dass die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender **Marktstandards** nicht dazu führt, dass der Einsatz von Verfahren ohne angemessenen Datenschutz beschlossen wird. In diesem Zusammenhang sei daran erinnert, dass das Bundesverfassungsgericht gerade die besondere Bedeutung der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben hat (1 BvR 370/07, 1 BvR 595/07, Urteil vom 27. Februar 2008). Der Arbeitskreis technische und organisatorische Datenschutzfragen hat deshalb bereits Kontakt zur KoSIT aufgenommen und seine Bereitschaft zur Mitarbeit und Unterstützung in diesem Gremium erklärt.

Ein weiterer Schwerpunkt der 4. Sitzung war das Thema IT-Sicherheit in Deutschland. Der IT-PLR hat sich am 3. März 2011 darauf verständigt, gemeinsam Rahmenbedingungen für die IT-Sicherheit von Bund, Ländern und Kommunen in einer **Leitlinie für Informationssicherheit** zu erarbeiten.

Eine Evaluierung der Gremienstrukturen und Abläufe ist seitens des IT-PLR vorgesehen. Eine Vorkonferenz zur vertieften inhaltlichen Vorbereitung des IT-PLR ist in der Diskussion. Es bleibt daher abzuwarten, ob eine solche Vorkonferenz auch die inhaltliche Auseinandersetzung mit datenschutzrelevanten Themen verbessern wird.

4.3 Zentraler IT-Dienstleister – Sachstand zum Landesrechenzentrum

In seinem IX. Tätigkeitsbericht (Nr. 4.2) hatte der Landesbeauftragte ausführlich von der Umsetzung des grundlegenden Kabinettbeschlusses der damaligen Landesregierung vom 14. November 2006 zur Bildung eines zentralen IT-Dienstleisters, dem **Landesrechenzentrum** (LRZ), berichtet und sich kritisch damit auseinandergesetzt sowie entsprechende Empfehlungen gegeben.

Wichtiger als die Entscheidung des Kabinetts zur Neuausrichtung der IT-Organisation und der Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei (IT-Strategie) und dem Ministerium des Innern (E-Government, Betrieb des Landesnetzes – ITN-LSA) war die zweite Entscheidung, nämlich der Auftrag an das Ministerium der Finanzen zur IT-Konsolidierung der Landesverwaltung und zum gleichzeitigen Aufbau des LRZ, unter datenschutzrechtlichen Gesichtspunkten, insbesondere in ihrer zukünftigen Auswirkung auf alle Ressorts des Landes Sachsen-Anhalt.

Der Landesbeauftragte hatte bereits im Mai 2009 im Rahmen des Workshops der Oberfinanzdirektion Magdeburg (OFD) bei der Vorstellung des Entwurfs einer Kabinettvorlage zum Geschäftsmodell „Landesrechenzentrum“, als den zukünftigen zentralen IT-Dienstleister des Landes, zum Thema Migration der IT-Querschnittsdienste/Übernahme von Fachverfahren auf die bestehenden restriktiven datenschutzrechtlichen Bestimmungen hingewiesen und eine diesbezügliche Berücksichtigung im Entwurf der Kabinettvorlage gefordert. Er hatte zugleich seine Unterstützung für die Begleitung dieses Migrationsprozesses angeboten. Eine weitere Information oder Beteiligung des Landesbeauftragten erfolgte allerdings nicht. Erst Ende August 2009 erreichte den Landesbeauftragten per E-Mail der Entwurf der Kabinettvorlage zum Geschäftsmodell für das LRZ.

Im Hinblick auf eine rechtzeitige Unterrichtungspflicht des Landesbeauftragten nach § 14 Abs. 1 Satz 2 DSG-LSA war das nicht akzeptabel. Nach Intervention des Landesbeauftragten beim Ministerium der Finanzen wurde ihm die Kabinettvorlage im November 2009 zur Verfügung gestellt. Den dazugehörigen Kabinettbeschluss erhielt der Landesbeauftragte aber nur „auszugsweise“.

In Zeiten des propagierten „Open Government/Open Data“ (vgl. Nr.1.3.4) hält der Landesbeauftragte diese Verfahrensweise der Landesregierung mittlerweile für anachronistisch, zumal er hier nicht aus reiner Neugier, sondern im Rahmen seines gesetzlichen Beratungsauftrages als Kontrollbehörde tätig wurde und damit seine unabhängige Amtsführung beeinträchtigt wird. Zeugt sie doch von einer gewissen Ignoranz in Bezug auf die Verpflichtung aller öffentlichen Stellen zur Unterstützung ihm gegenüber (§ 23 Abs. 1 DSG-LSA).

Unter diesem Gesichtspunkt wäre, im Hinblick auf die Unterrichtungspflicht aus § 14 Abs. 1 Satz 2 DSG-LSA, eine Anpassung der bisherigen Regelung im Abschnitt VI der Gemeinsamen Geschäftsordnung der Ministerien – Allgemeiner Teil (Zusammenarbeit der Ministerien, Beteiligung, §§ 37, 38, 40 GGO LSA I) zur besseren Beteiligung des Landesbeauftragten mit Beginn der 6. Wahlperiode durch die neue Landesregierung wünschenswert. So wie

in einer Kabinettvorlage ein „Gleichstellungspolitischer Bericht“ enthalten sein muss (§ 38 GGO LSA I), könnten zukünftig in einem „Datenschutz-Bericht“ etwaige Belange des Datenschutzes dargestellt werden.

Die Unterrichtung des Landesbeauftragten ist an keine Form gebunden. Im einfachsten Fall reicht also zur Erfüllung dieser Pflicht eine rechtzeitige Übersendung von Planungsunterlagen, u. a. auch von Entwürfen von Kabinettvorlagen, unter Hinweis auf eine Unterrichtung nach § 14 Abs. 1 Satz 2 DSG-LSA aus. Sie verursacht damit, im Gegensatz zu der dem Landesbeauftragten gegenüber oft geäußerten Meinung eines damit verbundenen „erheblichen zusätzlichen Aufwandes“, diesen eben nicht, sondern unterstützt seine gesetzliche Aufgabe, bereits im Planungsstadium bei Vorhaben der Landesregierung einen vorgezogenen Grundrechtsschutz zu gewährleisten. Zu diesen Vorhaben gehören zweifellos die IT-Konsolidierung der Landesverwaltung und der Aufbau des LRZ.

Mit der gegenwärtigen formalen Festlegung in § 40 GGO LSA I, den Landesbeauftragten nur zu beteiligen, soweit personenbezogene Daten verarbeitet werden, steht die Landesregierung selbst im Widerspruch zu Grundsätzen und Zielen in ihrer eigenen IT-Strategie, in der den Belangen des Datenschutzes und der Datensicherheit im Rahmen des IT-Managementprozesses durch rechtzeitige Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes zum Aufbau oder zur Änderung automatisierter Verfahren bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten entsprochen werden soll. Einem solchen IT-Managementprozess gehen bekanntermaßen Grundsatzentscheidungen in Form von Kabinettbeschlüssen voraus.

Der Kabinettbeschluss vom 1. September 2009 bestätigte die Vorlage des Ministeriums der Finanzen zum Geschäftsmodell des LRZ. Die darin u. a. aufgeführten mittelfristig nur noch durch das LRZ bereitzustellenden **IT-Querschnittschnittdienste** für über 300 Behörden innerhalb der Landesverwaltung

- zentraler User Help Desk (UHD), Benutzerbetreuung,
- zentrale Softwareverteilung,
- Terminal-Server-Technik,
- Virtualisierung (Server und Anwendungen),
- SAP-Kompetenz-Center,
- zentrale Datenspeicherung und -archivierung,
- Betrieb E-Mail-Infrastruktur/zentraler Verzeichnisdienst und
- Druck

lassen erkennen, dass die damit im Zusammenhang stehenden datenschutzrechtlichen Fragen nach wie vor der Erörterung und Beachtung bedürfen.

Das ist u. a. bei den Themen Auftragsdatenverarbeitung (§ 8 DSG-LSA), Wartung von Datenverarbeitungsanlagen oder -verfahren durch externe Dritte (§ 8 Abs. 7 DSG-LSA) sowie automatisierte Abrufverfahren (§ 7 DSG-LSA) in Verbindung mit der Vorabkontrolle bei automatisierten Verfahren (§ 14 Abs. 2 DSG-LSA) der Fall. Dem Datenschutz wurde in der Kabinettvorlage selbst kein und in der 37-seitigen Anlage A (Geschäftsmodell des LRZ) ein ganzer Satz gewidmet: *„Die bei den einzelnen Querschnitts- und Fachverfahren bestehenden datenschutzrechtlichen Bestimmungen und Regelungen werden bei der Übernahme der einzelnen Verfahren berücksichtigt bzw. eingehalten.“*

Das LRZ wurde aus dem Finanzrechenzentrum (FRZ) der OFD und dem ehemaligen Landesinformationszentrum (LIZ) in Halle als Abteilung 4 der OFD gebildet. Mit dem 1. September 2009 erfolgte gleichzeitig die Gründung des LRZ in dieser neuen Struktur. Die Zusammenführung des LIZ als LHO-Betrieb mit dem FRZ zum LRZ mit Hauptsitz in Halle (Saale) und einer Nebenstelle in Magdeburg erfolgte am 1. Januar 2010.

Der Projektbeirat, der vom Aufbaustab der sogenannten Stabsstelle „Konsolidierung des IT-Betriebes“ eingerichtet wurde, begleitete den IT-Konsolidierungsprozess beratend. Der Landesbeauftragte war Mitglied dieses Projektbeirates. In der 6. und letzten Sitzung des Projektbeirates im Mai 2010 wurde seiner Auflösung zugestimmt. Die Grundsatzentscheidung bezüglich der strukturellen Anbindung des LRZ in Form einer Verwaltungslösung an die OFD (Behördenmodell anstelle einer Anstalt des öffentlichen Rechts) machte diesen Projektbeirat quasi überflüssig.

Die Landesregierung hatte in ihrer Stellungnahme zum IX. Tätigkeitsbericht des Landesbeauftragten (LT-Drs. 5/2385) sehr knapp darauf verwiesen, dass der Aufbau des zentralen IT-Dienstleisters entsprechend dem Kabinettsbeschluss vom 14. November 2006 durch das Ministerium der Finanzen erfolgt. Inhaltlich wurde auf die Empfehlungen des Landesbeauftragten nicht eingegangen. *„Bei der technischen und organisatorischen Umsetzung durch das MF bzw. das LRZ wird auf die datenschutzkonforme Einrichtung und Übernahme der IT-Querschnittsdienste geachtet.“*, so die damalige Antwort der Landesregierung.

Die praktische Umsetzung der Migration der zentralisierbaren IT-Querschnittsdienste zum LRZ als ein wesentlicher Schritt zur IT-Konsolidierung innerhalb der Landesverwaltung hat das Ministerium der Finanzen für seinen Geschäftsbereich selbst als Pilotprojekt am 6. April 2010 abgeschlossen. Gleichzeitig nahm der zentrale User Help Desk im LRZ seinen Betrieb zur Nutzerbetreuung der migrierten Dienststellen auf.

Die dem Landesbeauftragten im Mai 2010 vom Ministerium der Finanzen angekündigte Kabinettvorlage zur Migration weiterer Ressorts liegt bisher nicht vor. Er soll aber bei der nächsten Ressort-Migration zur Bestandsaufnahme eingeladen und beteiligt werden. Der Vorteil des derzeitigen Migrationskonzepts je Behörde, welches eine Ist-Analyse, eine Konzepterstellung zur Ablösung der IT-Querschnittsdienste und danach die Übernahme dieser IT-Querschnittsdienste von der jeweiligen Behörde durch das LRZ vorsieht, liegt in der damit nur einmal notwendigen Befassung mit einer Behörde.

Eine grundsätzliche Entscheidung zum **Betrieb des zukünftigen Landesnetzes** (ITN XT – „eXTended“), anstelle des bisherigen Betriebes des Landesnetzes (ITN-LSA) durch das Technische Polizeiamt, steht immer noch aus und wurde auch in der damaligen Kabinettvorlage zum Geschäftsmodell des LRZ bislang von einer Übernahme durch das LRZ ausgenommen.

Mit dem "Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – vom 10. August 2009 (BGBl. I S. 2706) – IT-NetzG“ errichtet der Bund (gemäß § 1 IT-NetzG) zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. Das IT-NetzG wurde als Art. 4 des Gesetzes vom 10. August 2009 (BGBl. I S. 2702) vom Bundestag mit Zustimmung des Bundesrates beschlossen. Gemäß § 3 IT-NetzG erfolgt der Datenaustausch zwischen dem Bund und den Ländern über dieses Verbindungsnetz. § 3 des IT-NetzG tritt gem. Art. 13 Abs. 3 des Artikelgesetzes allerdings erst am 1. Januar 2015 in Kraft.

Hier bleibt abzuwarten, welche Entscheidungen das Ministerium der Finanzen als nunmehr zuständiges Ressort für die IT-Strategie und als Vertreter des Landes Sachsen-Anhalt im IT-PLR treffen wird. Nach fünf Jahren erfolgt nach der Aufteilung der Verantwortlichkeiten für die IT-Strategie, das E-Government und den zentralen IT-Dienstleister auf verschiedene Ressorts (s. VIII. Tätigkeitsbericht, Nr. 4.1) nunmehr mit Beginn der 6. Wahlperiode die Bündelung dieser Verantwortlichkeiten in einem Ressort, dem Ministerium der Finanzen. Damit verfügt das Land Sachsen-Anhalt nun erstmalig auch über einen „**IT-Beauftragten der Landesregierung**“, dessen Aufgaben ein Staatssekretär im Ministerium der Finanzen zukünftig im Sinne eines CIO wahrnehmen wird.

Die Staatskanzlei hat sich beim Landesbeauftragten im Mai 2011 für die vertrauensvolle Zusammenarbeit im Ständigen Staatssekretärsausschuss „Informationstechnologie“ zur Vorbereitung der bisherigen vier Sitzungen des IT-PLR bedankt. Der Landesbeauftragte setzt nach der Konzentration der Zuständigkeiten im Ministerium der Finanzen für die IT-Strategie, das E-Government und das LRZ auf eine ebenso vertrauensvolle wie effektive Zusammenarbeit. Seine frühzeitige Einbeziehung etwa im Rahmen der Entwicklung eines zentralen Personalmanagementsystems (PROMIS) lässt trotz noch zu lösender datenschutzrechtlicher und -technischer Fragestellungen (s. Nr. 18.2) auf eine gute Zusammenarbeit hoffen.

Zu einem der zukünftig zu behandelnden Themen gehört z. B. die Aufgabenstellung für das LRZ auf Basis des Beschlusses des IT-Koordinierungsausschusses vom 5. April 2011 zur zentralen Identitäts- und Zugriffsverwaltung der Landesverwaltung (IAM – Identity and Access Management). Das Ministerium der Finanzen wird durch diesen Beschluss aufgefordert, das LRZ mit der Ausschreibung auf der Basis der Arbeitsgruppe IT-Architektur der Landesleitstelle IT-Strategie der Staatskanzlei zu beauftragen. An den Ergebnissen der Arbeitsgruppe war auch der Landesbeauftragte als Mitglied beteiligt. Datenschutzrechtliche Belange sollten bereits bei der Ausschreibung durch das LRZ berücksichtigt werden (s. IX. Tätigkeitsbericht, Nr. 4.3).

4.4 E-Government-Maßnahmenplan 2010 – Fehlanzeige

Noch im Frühjahr 2010 wurde dem Landesbeauftragten seitens des Ministeriums des Innern eine Vorabbeteiligung zum E-Government-Maßnahmenplan 2010 des Landes avisiert. Auch die Staatskanzlei informierte den Landesbeauftragten auf seine Nachfrage zum Sachstand, dass im Mai 2010 seitens des Ministeriums des Innern eine Vorlage zur Mitzeichnung geplant sei. Allerdings war hier von der Fortschreibung einer „E-Government-Strategie des Landes“ und nicht mehr von einem E-Government-Maßnahmenplan 2010 die Rede. Denn nach dem am 29. April 2003 von der Landesregierung beschlossenen Grundkonzept E-Government in Sachsen-Anhalt (E-Government-Grundkonzept mit dem E-Government-Aktionsplan für die Landesverwaltung 2004-2010 und den sich daraus ergebenden Maßnahmenplänen 2005-2006, 2007 und 2008-2009) – der Landesbeauftragte berichtete hierzu regelmäßig in seinen vorangegangenen Tätigkeitsberichten (VII. Tätigkeitsbericht, Nr. 7.1; VIII. Tätigkeitsbericht, Nr. 4.2; IX. Tätigkeitsbericht, Nr. 4.5) – wäre eigentlich ein solcher E-Government-Maßnahmenplan auch für das Jahr 2010 zu erwarten gewesen.

Dafür erreichte den Landesbeauftragten auf seine Nachfrage hin im Juni 2010 ein erster **Entwurf** der „E-Government-Strategie des Landes Sachsen-Anhalt – Verwaltung 2020 – koordiniert, prozessorientiert und eigenverantwortlich handelnd“ (Stand: 22.06.2010). Unter Bezugnahme auf diesen Strategieentwurf sollte dem Landesbeauftragten danach ein E-Government-Maßnahmenplan 2010-2011 zur Vorabstimmung zugeleitet werden. Bei diesem Entwurfsstadium, für einen Zeitraum von 2010 bis 2020, ist es nach Kenntnis des Landesbeauftragten dann auch geblieben, der damals avisierte E-Government-Maßnahmenplan 2010-2011 liegt nicht vor und die für Juli 2010 vorgesehene Kabinettsbefassung fand nicht statt.

Im Resümee dieses Strategieentwurfs ging das Ministerium des Innern davon aus, dass von den bekannten 23 **E-Government-Leitprojekten** bereits 19 abgeschlossen sind und die restlichen vier sich in Umsetzung befinden bzw. zu Daueraufgaben geworden sind.

Eine wesentliche Ursache für die Nichteinbringung dieses Entwurfs dürfte in der am 24. September 2010 vom IT-Planungsrat in seiner 3. Sitzung verabschiedete **Nationalen E-Government-Strategie** (NEGS) liegen. Zur Ausarbeitung der NEGS wurde eine bis zum 31. Oktober 2010 befristete länderoffene Kooperationsgruppe „Strategie“ gebildet, in der auch das Ministerium des Innern vertreten ist. Deren Wirken wurde bis zum 30. Juni 2011 verlängert. Zukünftig geht es um die Umsetzung mit konkreten Maßnahmen zum Aufbau einer föderalen IT-Infrastruktur.

Positiv ist anzumerken, dass der erste Strategieentwurf des Ministeriums des Innern nach dem Vorbild der NEGS auch den Belangen des Datenschutzes zumindest in der Beschreibung des Zielsystems der E-Government-Strategie 2010-2020 eine entsprechende Bedeutung beimisst: *„Durch die fortschreitende Weiterentwicklung des E-Government können zielgruppenabhängig spezifische Risiken für die informationelle Selbstbestimmung entstehen. Um dieses Recht zu wahren, ist dem Datenschutz im Land Sachsen-Anhalt besondere Beachtung zu schenken.“*

An diesem Bekenntnis zur besonderen Beachtung des Datenschutzes wird auch die zukünftige E-Government-Strategie der neuen Landesregierung zu messen sein. Der Landesbeauftragte ist in diesem Zusammenhang bereit, wie bisher mit der Staatskanzlei und dem Ministerium des Innern, auch nach den strukturellen Veränderungen 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, die Zusammenarbeit fortzusetzen, um den Prozess der Verwaltungsmodernisierung weiterhin beratend zu begleiten.

4.5 Landesportal Sachsen-Anhalt

Das Landesportal (http://www.sachsen-anhalt.de) hat sich im Berichtszeitraum deutlich weiterentwickelt. Die Zugriffszahlen haben sich im Vergleich zu 2007 mehr als verdoppelt. 2010 gab es ca. 44,5 Millionen Zugriffe. Die Staatskanzlei hat eine Redaktionsrunde eingerichtet, in welcher sich der Landesbeauftragte nicht nur als Behörde beteiligt, sondern sich auch inhaltlichen datenschutzrechtlichen Aspekten widmet. Hierzu gehören beispielsweise Themen wie: SSL-Verschlüsselung von Webportalen mittels Zertifikaten, datenschutzgerechte Auslieferung von Videos im Landesportal und datenschutzgerechte Auswertung der Zugriffe auf das Landesportal.

SSL-Verschlüsselung von Web-Portalen

Der Landesbeauftragte wurde im Jahr 2010 durch Dritte mehrfach darauf hingewiesen, dass das Landesportal keine Absicherung durch SSL-Verschlüsselung und Zertifikate nutzt. Sowohl Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch Nutzern, welche Wert auf einen abgesicherten Zugriff legen, fiel das fehlende Zertifikat auf. Aus Kostengründen will die Staatskanzlei hier leider so schnell nichts ändern. Es gab jedoch eine Zusage, den Web-Mailer und auch den Zugang für Redakteure am Landesportal durch Zertifikate der Landes-PKI abzusichern. Damit werden personenbezogene Daten und schreibende Zugriffe auf die Datenbank über die Redaktionsschnittstelle besser geschützt. Dennoch ist ein Hinweis, dass die Verbindung fälschungs- und abhörsicher und mit dem richtigen Gegenüber aufgebaut wurde, sinnvoll. Auch gibt es nicht-personenbezogene Daten, die nur von einem Anbieter mit gesicherter Identität bezogenen werden sollten. Beispielsweise der PGP-Schlüssel des Landesbeauftragten. Die Webseiten des Landesportals sind auf Wunsch des Nutzers auch verschlüsselt auszuliefern. Dazu ist ein X.509-Zertifikat auf dem Webserver zu installieren, welches eine Auslieferung HTTPS-verschlüsselter Webseiten erlaubt. Im Browser wird das z. B. mit einem farbig hinterlegten Domainnamen oder einer solchen URL gekennzeichnet. Unsichere Adressen fallen dem Nutzer zunehmend auch auf. Leider ist ohne größere finanzielle Investition in ein Zertifikat einer bereits dem Webbrowser bekannten Zertifizierungsstelle (CA – Certificate-Authority) nur ein Minimalschutz möglich, indem preiswerte Zertifikate der Landes-PKI oder die von kostenfreien Anbietern genutzt werden. Bei allen preiswerten Lösungen ist die Absicherung der Zertifikate beim Importieren in den Webbrowser mangelhaft, da die sichere manuelle Beschaffung, Prüfung und Installation den Normalbenutzer häufig überfordert. Auch das ist ein Grund, warum die Wurzelzertifikate der Verwaltungs-PKI in den gängigen Webbrowsern von Haus aus hinterlegt werden

sollten. Die SSL-Schnittstellen sind mittlerweile freigeschaltet, jedoch verliefen Tests zur Nutzung der Verschlüsselung auf Rechnern in der Geschäftsstelle des Landesbeauftragten sowohl beim Web-Mailer als auch beim Redaktionssystem nicht erfolgreich. Aus diesem Grund versucht der Landesbeauftragte, durch kontinuierliches Aufgreifen des Themas u. a. in der AG Verwaltungs-PKI und damit auch beim BSI, die Wichtigkeit der Hinterlegung der Wurzelzertifikate der V-PKI in den Webbrowsern zu verdeutlichen und so über diesen Umweg dem Land die Nutzung der eigenen Landes-PKI für Webseiten zu ermöglichen. Viele Webseiten, angefangen von Google bis hin zur Wikipedia, ermöglichen es, ihre Dienste verschlüsselt zu nutzen. Das klappt noch nicht bei jedem Anbieter perfekt, aber die Entwicklung ist abzusehen, da Webserver-Zertifikate und verschlüsselte Datenübertragungen Stand der Technik sind. Spätestens mit der Einbindung von Open Data und Web 2.0-Funktionen direkt in das Portal werden Benutzerzugänge notwendig, und dann wird es nicht mehr ohne Verschlüsselung gehen.

Dass bei der Nutzung von HTTPS/SSL weltweit Defizite herrschen, ist auch Projekt-Thema der Internet Engineering Task Force. Diese will mittels HTTP Strict Transport Security (HSTS) die Verschlüsselung standardisieren. Konkret nutzen viele Webseiten nur auf wenigen Seiten – etwa zum Anmelden – Verschlüsselung und schalten im Anschluss wohl wegen Performance-Bedenken auf unverschlüsselten Betrieb zurück. HSTS-fähige Server erlauben es, Nutzer aktueller Browser (z. B. Firefox, Chrome) zur durchgehenden Verschlüsselung zu zwingen. Der Server sendet hierzu eine Kennung („ich kann HSTS“) zusammen mit der Sitzungslaufzeit, für welche verschlüsselt werden soll. Der Browser wird nun eine durchgehende Verschlüsselung sicherstellen und auch Verweise auf servereigene Seiten mittels HTTP-Protokoll automatisch nach https korrigieren.

Aber auch die Browser-Hersteller müssen dazu angeregt werden, Zertifikate kontrollierbarer zu hinterlegen. In den Browsern selbst sind unzählige CAs hinterlegt und es ist unmöglich, einen Überblick über die Vertrauenswürdigkeit aller CAs zu erlangen. Was weiß ein Nutzer schon über eine CA irgendwo am anderen Ende der Welt? Wird diese überhaupt benötigt? Hier könnte die Verteilung der Wurzelzertifikate z. B. mittels Profilen geregelt werden. Wer der Verwaltung vertraut, kann diese aktivieren, wer nur großen Unternehmen vertraut, kann sich diese gebündelt installieren. Lokale Anbieter könnten dynamisch bei Bedarf oder sogar webseitenbezogen freigeschaltet werden, sodass die Menge der CAs die immer aktiv ist, überschaubar bleiben würde.

Neue Inhaltselemente im TYPO3

Im Landesportal selbst wurden im Rahmen einer Aktualisierung des TYPO3 neue Inhaltselemente freigeschaltet. Hier wurde bereits in den frühen Phasen in der Redaktionsrunde darauf hingewiesen, dass Google bzw. YouTube ggf. durch das Videoelement unbemerkt Daten der Besucher weitergeleitet bekommen, obwohl diese gar nicht das Video abspielen. Dieses Problem ist z. B. auch bei der Einbindung von Twitter und FaceBook in eigene Webseiten vorhanden. Möglich ist, das Startbild des Videos als Grafik auf dem eigenen Webserver zu hinterlegen und ggf. einen Hinweis einzublenden, ob wirklich Daten vom externen Anbieter nachgeladen werden sollen. Letztlich hat

sich das Land – vorbildlich – dafür entschieden, die Videos komplett im Landesportal zu hinterlegen und über ein ebenfalls hinterlegtes Abspielprogramm zu präsentieren. Videos können via Plugin im Landesportal genutzt werden – entweder als YouTube-Video mit der entsprechenden Film-Nummer oder als Flash-Video (FLV) auf dem Landesportal. Die Auslieferung des Videos vom eigenen Webserver ist die datenschutzgerechte Lösung. Ein YouTube-Video zum Test war jedoch nicht auffindbar.

Nutzung aktueller Web-Standards

Der Versuch, die Webseiten nach aktuellen Web-Standards ausliefern zu lassen, scheiterte. Der aktuelle „XHTML 1.0 Transitional“-Standard der Website (und der wird noch nicht einmal erfüllt) aus dem Jahr 2000 ist eine Neuformulierung des HTML4-Standards in XML. Jede Weiterentwicklung des Landesportals hin zu XHTML 1.1 (Empfehlung des W3C zur Nutzung erfolgte bereits im Jahr 2001) blieb aus. Es ist bis heute keine syntaktische Überprüfbarkeit der Website möglich, da zu viele Fehler enthalten sind. Laut Aussage des Portal-Betreibers soll es so bleiben, da der Internet Explorer 6 (laut Wikipedia „Webbrowser“ derzeit mit 1,6% Marktanteil, Stand 05/2011) unbedingt unterstützt werden muss. Das sieht der Landesbeauftragte nicht so. Für auszuliefernde Webseiten ist mindestens XHTML 1.1 als Format zu nutzen. Vereinzelt anzutreffende Uralt-Browser können daraus abgeleitete, angepasste HTML-Dokumente erhalten. Auch eine ausschließliche Formatierung per CSS ist sinnvoll. Das Layout sollte schnellstmöglich komplett auf Nutzung von CSS umgestellt werden, da erst dadurch sauberer HTML-Code und die Nutzung aktueller Standards möglich werden. Das kommt der Benutzbarkeit der Website im Allgemeinen zugute. Derzeit erzeugt der automatische Editor sehr viele Formatanweisungen selbst. Damit ist leider keine einfache Wiederverwendbarkeit von Daten des Landesportals realisierbar. Da diese nicht personenbezogener Art sind, wurde die Standardisierung an dieser Stelle jedoch nicht weiter verfolgt.

Datenschutzgerechte Auswertung der Zugriffe auf das Portal

Die Informationen der bisherigen Loganalyse-Software Sawmill reichten nicht aus, da diese nur TYPO3-Logs auswerten konnte. Google Analytics sollte nicht genutzt werden (vgl. Nr. 14.6). Die Wahl fiel auf Piwik. Fast alle Landkreise wurden mittlerweile auf Piwik umgestellt und haben bereits erste Erfahrungen gesammelt. Sawmill und Piwik laufen derzeit parallel, um Vergleichswerte zu erhalten.

4.6 EU-Dienstleistungsrichtlinie – eine Bestandsaufnahme

Die Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt – EU-Dienstleistungsrichtlinie (EU-DLR) – (ABl. EU Nr. L 376 S. 36) in Sachsen-Anhalt erfolgte federführend durch das Ministerium für Wirtschaft und Arbeit, deren IT-Umsetzung durch das Ministerium des Innern. Zum Einheitlichen Ansprechpartner (EA) nach Art. 6 der EU-DLR in Sachsen-Anhalt wurde mit Kabinettbeschluss vom 23. September 2008 das Landesverwaltungsamt bestimmt.

Der Landesbeauftragte wurde in diesen Umsetzungsprozess von beiden Ministerien rechtzeitig informiert und beteiligt. Durch seine Mitarbeit in den dazu gebildeten Arbeitsgruppen fanden rechtliche wie technische Anforderungen des Datenschutzes eine entsprechende Berücksichtigung (IX. Tätigkeitsbericht, Nr. 4.7).

Die Kommunikation des EA und der zuständigen Behörden mit den Behörden der europäischen Mitgliedstaaten erfolgt mittels IMI-Basismodul EU-DLR (Internal Market Information System – IMI) im sogenannten Koordinierungsmodell. Als IMI-Behörden wurden nach dem Koordinierungsmodell die Landkreise und kreisfreien Städte und ergänzend die Kammern registriert, soweit sie fachlich oder fachaufsichtlich zuständig sind. Der Vorteil des Koordinierungsmodells, auch aus datenschutzrechtlicher Sicht, liegt im Wegfall des zentralen Eingangs von Anfragen beim EA. Damit gehen Anfragen direkt an die zuständigen Behörden.

Für diese IT-Lösung wurden sowohl Basiskomponenten gemäß Rahmenvereinbarung zwischen dem Land Sachsen-Anhalt und den Kommunen genutzt, u. a. auch das Elektronische Gerichts- und Verwaltungspostfach (EGVP) zur Kommunikation. Neubeschaffungen wurden nur für das Service-Portal, das Registrierungs- und das Authentifizierungsmodul sowie das Fallmanagement für den EA und die zuständigen Behörden durchgeführt. Das Betriebskonzept für die technische Umsetzung im Landesrechenzentrum (LRZ) basiert auf dem IT-Umsetzungskonzept zur EU-DLR des MI (Stand: 8. April 2009).

Mit der noch rechtzeitigen Verabschiedung des Gesetzes zur Umsetzung der europäischen Dienstleistungsrichtlinie in Sachsen-Anhalt vom 16. Dezember 2009 (GVBl. LSA S. 700) konnte die vorgegebene Umsetzungsfrist der EU-DLR bis zum 31. Dezember 2009 eingehalten werden.

Artikel 1 dieses Gesetzes ist das **Einheitlicher-Ansprechpartner-Gesetz** (EAG LSA). In ihm werden Regelungen zum EA, der europäischen Verwaltungszusammenarbeit und zur verwaltungskostenrechtlichen Umsetzung der EU-DRL getroffen. Nach § 6 Abs. 1 EAG LSA sind der EA und die zuständigen Behörden zur Zusammenarbeit verpflichtet, die in der Regel auf elektronischem Weg, mit Ausnahme der „Verbundenen Verfahren“ erfolgt. Die Zusammenarbeit des EA mit den zuständigen Behörden hat die Landesregierung gemäß § 6 Abs. 2 EAG LSA durch Verordnung zu regeln. In dieser Verordnung wären u. a. Vorgaben zur Sicherstellung der elektronischen Verfahrensabwicklung und der elektronischen Kommunikation sowie die Befugnisse zum Datenzugriff und dem Datenaustausch zu regeln. Die Landesregierung hat diese Verordnung bisher nicht erlassen.

Im darauffolgenden Jahr hat der Landesbeauftragte bewusst bei den dafür zuständigen Behörden auf formelle Kontrollen verzichtet. Erst im Frühjahr 2011 führten ihn Informationsbesuche bezüglich des praktischen Umsetzungsstandes zum EA in das Landesverwaltungsamt sowie das für die IT-Umsetzung zuständige LRZ nach Halle.

Als Ergebnis der Informationsbesuche ist festzustellen, dass das System sehr zurückhaltend genutzt wird. Nur zwei Dienstleistungserbringer haben im

Jahr 2010 den Versuch unternommen, über den EA ihre Anträge elektronisch abzuwickeln.

18 Dienstleistungserbringer haben sich seither am EA-Portal registriert. Die Mehrheit der Anfragen erreicht den EA als E-Mail und wird entsprechend beantwortet oder zur Beantwortung an die zuständige Behörde weitergeleitet. Im Jahr 2010 erfolgten vermehrt Informationszugriffe auf das EA-Portal. Die Zugriffsstatistik (Pageviews: 2009: 2649; 2010: 26392; 2011(I. Q.): 7987) ist dafür ein Beleg.

Der EA ist zugleich IMI-Koordinator. Als sogenannte Verbindungsstelle nach Art. 28 Abs. 2, Art. 29 Abs. 3 und Art. 32 Abs. 1 der EU-DLR wurde noch keine Vorwarnung veranlasst. Der sogenannte „Vorwarnungsmechanismus“ (bei ernster Gefahr für die Gesundheit oder die Sicherheit von Personen oder die Umwelt durch einen Dienstleistungserbringer) wurde von deutschen Behörden bisher nicht genutzt. Auch aus den EU-Mitgliedstaaten trafen bisher keine Vorwarnungen ein. Durch die zuständigen Behörden (Landkreise und kreisfreie Städte, Kammern) wurden 14 Anfragen an die EU-Mitgliedstaaten über das Modul IMI-EU-DLR gestellt.

Bei der IT-Umsetzung im LRZ besteht allerdings nach Einschätzung des Landesbeauftragten hinsichtlich des Betriebskonzepts EU-DLR und der Aufgabenbeschreibung (Vers. 0.8, 2. Dezember 2009) Handlungsbedarf. Das betrifft vor allem das noch fehlende Sicherheitskonzept, welches die Grundlage für die Umsetzung von Datenschutz und Datensicherheit bilden soll, im Betriebskonzept aber nur auf dem Papier existiert. Hier sieht der Landesbeauftragte auch das zuständige Ministerium des Innern als Auftraggeber in der Pflicht. Als eigentlicher Betreiber des EA-Portals des Landes hat es die Betreuung des Portals durch das LRZ zusammen mit Fremdfirmen konzipiert. Beim Betrieb und der Wartung des modular aufgebauten Gesamtsystems tragen auch diese externen Dritten für einzelne der von ihnen betreuten Komponenten die Verantwortung für die Systemsicherheit. Inwieweit bei der Vertragsgestaltung mit diesen externen Anbietern datenschutzrechtliche Belange ausreichend (auch vertraglich) berücksichtigt wurden, ist dem Landesbeauftragten nicht bekannt. Zu verweisen ist hier in erster Linie auf die Regelungen zur Auftragsdatenverarbeitung und deren Beachtung (§ 8 DSG-LSA).

Auch wenn aus nachvollziehbaren zeitlichen Gründen und Zwängen bei der technischen Umsetzung der EU-DLR die Ausarbeitung eines umfassenden Sicherheitskonzepts zum damaligen Zeitpunkt zurückgestellt wurde, ist das nunmehr nachzuholen. Der Landesbeauftragte ist bereit, das Ministerium des Innern und das LRZ bei Bedarf dabei zu unterstützen. Gleiches gilt für die Ausarbeitung der Verordnung nach § 6 Abs. 2 EAG LSA durch das Wirtschaftsministerium.

4.7 Binnenmarktinformationssystem IMI – Sachstand

Neben der Umsetzung der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22) (Berufsanerkennungsrichtlinie) wird dieses System (IMI-Modul EU-DLR) mit Beginn des Jahres 2010 ebenfalls zum Informationsaustausch bei der Umsetzung der Richtlinie

2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (ABl. EU Nr. L 376 S. 36) (EU-Dienstleistungsrichtlinie – EU-DLR) in Sachsen-Anhalt durch die zuständigen Behörden genutzt.

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 4.8) die Probleme bei der Umsetzung des Binnenmarktinformationssystems IMI (Internal Market Information System) dargestellt. Die Europäische Kommission (KOM) betreibt dieses System selbst und stellt es den EU-Mitgliedsstaaten kostenlos zur Verfügung. Grundsätzlich soll es die Verwaltungszusammenarbeit in der Europäischen Union (EU) wesentlich vereinfachen und verbessern und zukünftig für weitere Rechtsbereiche genutzt werden. Unterschiedliche Auffassungen zur Notwendigkeit einer spezifischen Rechtgrundlage für das IMI bestehen aber zwischen der KOM und den Datenschutzbeauftragten. Die Forderung, dieses komplexe Informationssystem zur europäischen Verwaltungszusammenarbeit auf eine tragfähige Rechtsgrundlage zu stellen, besteht nach wie vor (IX. Tätigkeitsbericht, Anlage 14, Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4. April 2009 zur Umsetzung des Binnenmarktinformationssystems IMI).

Nach der Stellungnahme des Europäischen Datenschutzbeauftragten und in Abstimmung mit den Datenschutzbeauftragten und der Art. 29 Arbeitsgruppe hatte sich die KOM auf einen Kompromiss verständigt, der mit Hinblick auf die fehlende Rechtsgrundlage für das IMI ein schrittweises Vorgehen zur Lösung dieses Problems vorsah. Der Landesbeauftragte hatte die damalige Situation mit dem Ministerium für Wirtschaft und Arbeit im April 2009 erörtert und als datenschutzrechtliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten im IMI-System eine modifizierte informierte Einwilligung gemäß § 4 Abs. 2 DSG-LSA empfohlen. Dieser Empfehlung war das Ministerium für Wirtschaft und Arbeit gefolgt und hatte alle beteiligten IMI-Behörden des Landes entsprechend informiert.

Bis zum Ende 2009 erfolgten danach durch die EU-Mitgliedsstaaten aufgrund der im IMI gesammelten Erfahrungen Rückmeldungen zu den Datenschutzleitlinien der KOM vom 23. März 2009 und zu deren praktischer Anwendbarkeit. Die Landesdatenschutzbeauftragten hatten in einer gemeinsamen Stellungnahme nachdrücklich ihre grundsätzliche Forderung bekräftigt, dass der Betrieb des IMI auf eine ausreichende Rechtsgrundlage zu stellen ist. Vorsorglich wurde in diesen Zusammenhang nochmals in Bezug auf die neuen Vorschriften des Verwaltungsverfahrensgesetzes (VwVfG) zur europäischen Verwaltungszusammenarbeit festgestellt, dass die Amtshilfebestimmungen der §§ 8a ff. VwVfG keine datenschutzrechtliche Befugnisnorm darstellen. Die damaligen Datenschutzleitlinien der KOM verwiesen selbst mit Hinweis auf Artikel 7 c) und e) der Richtline 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (EU-DSRL) auf notwendige Rechtsgrundlagen für eine Datenverarbeitung.

Hatte sich die KOM in ihrem Bericht über den Stand des Datenschutzes im IMI vom 22. April 2010 noch zufrieden bezüglich der dazu getroffenen Regelungen gezeigt, ist nunmehr Bewegung in die Diskussion um eine tragfähige

Rechtsgrundlage gekommen. Auslöser könnte u. a. die Anfrage des Bundesratsbeauftragten eines Landes in der beratenden Arbeitsgruppe der KOM zum IMI-Modul der EU-DLR an den Vorsitzenden des Arbeitskreises Grundsatzfragen der Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Juni 2010 gewesen sein, mit der gleichzeitigen Bitte um Unterstützung bei der Beantwortung der datenschutzrelevanten Fragen.

Der Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung hat diesen Fragenkomplex auf seiner Sitzung im September 2010 behandelt und dem Bundesratsbeauftragten im Oktober 2010 geantwortet.

Für eine Vorabkontrolle (gem. Art. 20 EU-DSRL) bestehen in den Länder unterschiedliche Regelungen. Bei einer beabsichtigten gesetzlich verbindlichen Einführung des IMI-Systems wäre aber nach Meinung des Landesbeauftragten diese Vorabkontrolle grundsätzlich entbehrlich.

Grundsätzlich bestehen beim IMI keine Zweifel an der Datenschutzkonformität in technischer Hinsicht. Mit Hinweis auf die bisher nicht erfolgte Bereitstellung eines Sicherheitskonzepts für IMI, seiner technischen Verfahrensbeschreibung sowie von Testergebnissen der KOM an die Mitgliedsländer bzw. die Datenschutzbeauftragten hat sich der Arbeitskreisvorsitzende an den Europäischen Datenschutzbeauftragten (EDSB) gewandt und um Unterstützung bzw. Vermittlung gebeten. Die KOM verweist im Bezug auf das IMI-System darauf, nur der datenschutzrechlichen Kontrolle des EDSB zu unterliegen.

Weiter wurde in der Antwort klargestellt, dass die §§ 8a ff. VwVfG allgemeine Verfahrensbestimmungen und eben keine Befugnisnorm für eine Datenverarbeitung darstellen. Das Verfahren IMI würde bei einer innerstaatlichen Anwendung, für die es in anderen Bundesländern scheinbar Überlegungen gibt – in Sachsen-Anhalt nach Auskunft des Ministeriums für Wirtschaft und Arbeit aber nicht – den durch die Datenschutzgesetze in den Ländern und beim Bund vorgegebenen Prüfbestimmungen unterliegen.

In der nunmehr dem Landesbeauftragten vorliegenden Mitteilung der Europäischen Kommission vom 21. Februar 2011 bezüglich einer Strategie für den Ausbau und die Weiterentwicklung des Binnenmarktinformationssystems IMI ist erkennbar, dass die KOM damit ihre Auffassung zur Notwendigkeit einer eigenen Rechtsgrundlage für das IMI geändert hat und beabsichtigt, noch im Jahr 2011 ein Rechtsinstrument vorzuschlagen.

Der Landesbeauftragte wird die Entwicklung weiter verfolgen und dabei den bewährten Kontakt zum Wirtschaftsministerium zur gegenseitigen Information und zur Erörterung datenschutzrechtlicher Fragen halten.

4.8 De-Mail

Mit dem De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666) soll der Aufbau einer Infrastruktur für eine sichere und vertrauensvolle elektronische Kommunikation im Rechts- und Geschäftsverkehr vorangetrieben werden. Diese dient der Verbesserung des Sicherheitsniveaus gegenüber herkömmlichen E-Mails, von denen derzeit mehr als 95% unverschlüsselt und abfangbar

transportiert werden. Bereits im IX. Tätigkeitsbericht (Nr. 4.11) wurden erste Entwicklungen der De-Mail aufgegriffen. Im Februar 2009 wurde mit dem Bürgerportalgesetz die Einrichtung einer sicheren, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) überwachten, Kommunikationsplattform und deren Nutzung durch den Bürger unter Zuhilfenahme des neuen Personalausweises (nPA) beschlossen. Die Bundesregierung legte im Oktober 2010 einen Entwurf für ein "Gesetz zur Regelung von De-Mail-Diensten" vor, welches den Rechtsrahmen für private De-Mail-Anbieter regeln sollte. Der Bundesrat nahm zum Jahresende Stellung und forderte umfangreiche Verbesserungen, welche hauptsächlich den Datenschutz betrafen. Die Forderungen werden vom Landesbeauftragten unterstützt.

Das wichtigste Merkmal einer De-Mail ist die Verbindlichkeit. Bei der Beantragung eines De-Mail-Kontos wird die Identität des Antragstellers überprüft. Da Absender und auch Empfänger eindeutig identifizierbar sind, ist der systematische Missbrauch wie etwa das Versenden von Spam oder Nachrichten mit gefälschtem Absender unmöglich. Dennoch gibt es verschiedene Kritikpunkte. Nicht alle sind in jedem Fall relevant. So wird häufig kritisiert, dass De-Mail keine anonyme Nutzung zulässt. Man muss dabei bedenken, dass das System der Kommunikation mit Behörden dient, welche ihre Antragsteller in der Regel kennen müssen, um auf Anfragen sinnvoll eingehen zu können. Anonyme Anfragen sind insbesondere für einfache Auskünfte vorstellbar, jedoch ist eine vollständig anonyme Einlieferung von De-Mails wie im E-Mail-System schon aus Gründen des Spamschutzes nicht möglich. Insofern muss der Nutzer sich darüber im Klaren sein, dass De-Mail eben kein absolut anonymes Netzwerk ist. Der Landesbeauftragte hält die Möglichkeit des Versendens von anonymen Mitteilungen von einem De-Mail-Postfach aus dennoch für sinnvoll. Hauptkritikpunkt des De-Mail-Systems ist, dass De-Mails zwar verschlüsselt transportiert und ebenso auf den Servern der Anbieter gelagert werden, zur Viren- und Spamprüfung aber kurzzeitig entschlüsselt werden sollen. Das ist weder notwendig noch datenschutzgerecht, da ein missbräuchlicher Zugriff auf die De-Mails so nicht ausgeschlossen werden kann.

Leider konnte sich nicht auf ein einheitliches Kennzeichen von De-Mail-Adressen geeinigt werden. Der Dienst soll anhand der verwendeten De-Mail-Adresse sowohl auf den Anbieter als auch auf die De-Mail-Konformität hinweisen. Die Aufnahme des Anbieternamens in die Adresse wird den Transfer von De-Mail-Konten zu anderen Anbietern verhindern bzw. einen Umzug von einem Anbieter zu einem anderen Anbieter erheblich erschweren. Eine sinnvolle Regelung wäre es, De-Mail-Adressen zentral in anbieterneutraler Form zuzuteilen. Dies würde auch eine dauerhafte Identifikation des Anwenders mit „seiner“ Adresse gewährleisten können. Die vom Bundesrat geforderte Abstimmung des Verfahrens mit dem Signaturgesetz ist obligatorisch. Hier muss eine derartige Umsetzung realisiert werden, welche die bestehenden Kryptografieverfahren nicht verwässert, gleichzeitig aber die Rechtsfolgen für die De-Mail-Nutzung klar definiert. Eine Portierbarkeit von Dokumenten zwischen den einzelnen Diensteanbietern ist wünschenswert. Auch die vom Bundesrat geforderte Verpflichtung akkreditierter Diensteanbieter, den Zugriff des De-Mail-Nutzers auf sein Konto durch eine Anmeldung mit mindestens zwei voneinander unabhängigen Sicherungsmitteln sicher zu gestalten, statt nur auf die gängige Verwendung von Benutzername und Passwort zu set-

zen, ist als Stand der Technik unumgänglich. Das wäre mit Nutzung des neuen Personalausweises sogar einfach realisierbar.

Offen ist derzeit insbesondere die Frage der zwingenden Erforderlichkeit einer **Ende-zu-Ende-Verschlüsselung**. Der jeweilige Schutzbedarf personenbezogener Daten ist immer wirksam mittels technisch-organisatorischer Maßnahmen zu gewährleisten. Im Einzelfall sind damit auch De-Mails durch geeignete Maßnahmen sicherheitstechnisch aufzuwerten, sofern das bereits höhere De-Mail-Sicherheitsniveau nicht dem den Daten angemessenen Schutzbedarf entspricht. Damit kann für die Übermittlung von Daten mit höherem Schutzbedarf auch eine Ende-zu-Ende-Verschlüsselung erforderlich werden.

Bleibt hierzu noch die Betrachtung der Realisierbarkeit. Die Begründung, dass der Verzicht auf eine durchgehende Ende-zu-Ende-Verschlüsselung aus Gründen des Virenschutzes und der dazu notwendigen Entschlüsselung notwendig sei, ist nicht haltbar. Auch das BSI weist darauf hin, dass eine Ende-zu-Ende-Verschlüsselung bei De-Mail einfach realisierbar ist und die Schlüssel sogar einfach im öffentlichen Verzeichnisdienst hinterlegt werden können. Ebenso könnte eine Virenprüfung auf dem Rechner des De-Mail-Anbieters zum Zeitpunkt des Abrufs der De-Mail bei Eingabe eines Passworts zum geheimen Benutzerschlüssel erfolgen und die De-Mail anschließend nur per Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS) transportverschlüsselt übertragen werden. Das wäre strenggenommen keine richtige Ende-zu-Ende-Verschlüsselung, weil der Schlüssel auch hinterlegt werden würde, aber das würde den Zugriff auf die E-Mails nicht völlig offen lassen, da er jeweils gezielt mit einer Anmeldung des Nutzers am System verbunden und so freigeschaltet werden müsste. Vorteil wäre, dass die Virenprüfung jeweils mit aktuellen Signaturen erfolgen würde. Die Sicherheit der De-Mail wäre immer noch direkt abhängig vom Vertrauensstatus des Providers, also ob Passwörter im Profil hinterlegt werden oder sofort nach Ablauf der Sitzung wieder vergessen werden oder der Provider gar anderen Behörden Zugriff gewährt. Aber ist ein Mehr an Sicherheit gegenüber dem Provider im WebMail-Kontext überhaupt realisierbar? Diese Variante böte zusätzlich die Möglichkeit einer echten Ende-zu-Ende-Verschlüsselung, wenn sich der kryptografische Schlüssel im Hoheitsbereich des Nutzers befindet. Dann wäre kein Virenschutz und ggf. kein Zugriff per Web-Schnittstelle möglich, aber das wäre in diesem Zusammenhang auch gar nicht erforderlich, da der Nutzer entweder weiß, was er tut (wenn er manuell verschlüsselt) oder die entsprechenden Daten in seinem E-Mail-Programm hinterlegt hat und auch in diesem Fall das System des Nutzers für Schutzmaßnahmen verantwortlich ist. Technisch denkbar wäre auch, dass der De-Mail-Ersteller oder ein von diesem beauftragter Dritter kryptografisch beglaubigt, dass die De-Mail nur bestimmte Inhalte aufweist; also beispielsweise nur Textzeichen enthält, oder dass eine Grafik oder eine PDF-Datei mit einem bestimmten Generator in einem bestimmten Format gespeichert wurde. Damit könnte ein Finanzamt z. B. Bescheide herausgeben, die nicht entschlüsselt werden müssten, da eine separate Signatur existiert, die die Unbedenklichkeit des verschlüsselten Inhalts bescheinigt.

Aus Spamschutzgründen auf Sicherheit zu verzichten, ist ebenso wenig vernünftig. Da sowohl die Identität des Nutzers als auch des Dienstleisters, der

De-Mail ins System eingespeist hat, bekannt sind, sollte es ohne Mehraufwand möglich sein, möglichen Spam von Dritten bspw. durch Filterung auch ohne Entschlüsselung Einhalt zu gebieten. Auch Behörden-Spam darf es nicht geben. Dieser wäre bei Auftreten sofort – ggf. auch administrativ – zu unterbinden.

Eine Nutzung von Ende-zu-Ende-Verschlüsselung ist ohne Komforteinbußen auch für Nutzer, denen die Möglichkeit zu vorbereitenden Aktivitäten auf den eigenen Rechnern fehlt, durch die De-Mail-Dienstleister ohne Mehraufwand anbietbar. Selbst einer echten Ende-zu-Ende-Verschlüsselung steht prinzipiell nichts im Wege, sofern der Nutzer mit der ggf. nicht möglichen und bei entsprechenden Zusatzmaßnahmen auf Absender- und Providerseite auch nicht erforderlichen Spam- und Virenprüfung einverstanden ist. Die Schlüssel könnten einfach im Verzeichnisdienst hinterlegt werden. Damit gibt es aus technischer Sicht gar keinen Bedarf, ein niedrigeres Sicherheitsniveau als Ende-zu-Ende-Verschlüsselung überhaupt in Erwägung zu ziehen. Hier sind die De-Mail-Anbieter in der Pflicht, entsprechende Angebote bereitzustellen, der Gesetzgeber sollte Ende-zu-Ende-Verschlüsselung wie beschrieben als Mindeststandard vorschreiben.

Anbieter von De-Mail sind derzeit 1&1, GMX.de, Web.de, die Deutsche Post AG und die Deutsche Telekom. Die Deutsche Post AG stieg aus dem De-Mail-Projekt aus, baut jedoch mit dem E-Post-Brief ein ebensolches System auf, welches später auch eine Zulassung als De-Mail-Dienstleister erhalten soll.

Das De-Mail-Gesetz wurde im März 2011 trotz heftiger Kritik mit nur wenigen Änderungen beschlossen. Die geforderte Ende-zu-Ende-Verschlüsselung wurde nicht aufgegriffen. Jedoch soll darüber informiert werden. Auch die Entscheidung zur Datenbereitstellung in einem Verzeichnisdienst liegt nun beim Nutzer. Der Bürger hat des Weiteren ein Wahlrecht, ob er die De-Mail-Adresse zur Nutzung freigeben will oder nicht. Die Präsenz der Adresse im Verzeichnisdienst ist keine Zustimmung zur Nutzung durch öffentliche Stellen.

Stellen, die einen De-Mail-Zugang anbieten, sollten auch einen Ende-zu-Ende verschlüsselten Zugang vorsehen. Schließlich entscheidet allein der Nutzer durch Kontaktaufnahme, welches Sicherheitsniveau angemessen ist. Ohne Wahlmöglichkeit würde dieser ggf. zu einer zu niedrigen Stufe gezwungen werden. Das darf aber nicht sein. Aus datenschutzrechtlicher Sicht ist eine Ende-zu-Ende-Verschlüsselung bei der Kommunikation die beste Lösung.

Als Fazit lässt sich sagen, dass De-Mail eine sinnvolle Ergänzung zu herkömmlichen E-Mails und Briefen darstellt. Sie ist jedoch keine 1:1-Nachbildung des Briefes und somit auch kein in jedem Fall nutzbarer Ersatz für diesen. Die neu gewonnenen Vorteile der De-Mail, wie eine eindeutige Identifizierbarkeit aller Beteiligten, sind gleichzeitig auch die Nachteile und es ist sinnvoll, nicht alle Möglichkeiten moderner Datenverarbeitung zu erlauben und umzusetzen. De-Mail kann zu Datenschutzverletzungen führen. Ein normaler Brief in der Wohnung ist besser vor dem Zugriff Dritter geschützt als eine De-Mail. Eine solche Zugriffsmöglichkeit auf De-Mails beim Anbieter

bedeutet auch den Verzicht auf Rechte des Betroffenen, die bisher nicht zur Diskussion standen.

5 Ausländerangelegenheiten

5.1 Errichtung einer Visa-Einlader- und Warndatei – Weiterentwicklung

Bereits in seinem IX. Tätigkeitsbericht (Nr. 6.1) hat sich der Landesbeauftragte mit einem Gesetzentwurf zur Errichtung einer Visa-Einlader- und Warndatei befasst. Wie zum damaligen Zeitpunkt zu erwarten war, ist ein solches Vorhaben von der damaligen Bundesregierung nicht verabschiedet worden.

Im Koalitionsvertrag für die 17. Wahlperiode wurde zwischen Union und FDP vereinbart, eine Visa-Warndatei zu errichten.

In dieser Datei sollen die Daten der Bürger gespeichert werden, die im Zusammenhang mit rechtswidrigen Handlungen im Visaverfahren, so z. B. als Visa-Betrüger, Menschenhändler oder Menschen, die durch ein Einreisevergehen aufgefallen sind, gespeichert werden. Dabei ist jedoch unklar, ob in dieser Datei nur verurteilte Straftäter oder auch Verdachtsfälle gespeichert werden. Sollte dies der Fall sein, bestünde die Gefahr, dass auch Menschen in dieser Datei gespeichert werden, welche auffällig oft Ausländerinnen und Ausländer einladen.

Im April 2011 wurde durch den Bundesinnenminister mitgeteilt, dass das Bundeskabinett Eckpunkte für ein Visawarndateigesetz sowie für ein Verfahren eines Datenabgleichs für Sicherheitszwecke beschlossen habe.

Dem Landesbeauftragten ist ein Referentenentwurf eines Gesetzes zur Errichtung einer Visa-Warndatei und zur Änderung des Aufenthaltsgesetzes mit Stand 5. Mai 2011 durch die anderen Datenschutzbeauftragten zur Kenntnis gegeben worden. Eine Stellungnahme des Landesbeauftragten an das Ministerium des Innern war zu diesem Zeitpunkt jedoch schon nicht mehr möglich, da die Frist zur Stellungnahme der Länder bereits am nächsten Tag ablief.

Bei diesem Entwurf ist aus datenschutzrechtlicher Sicht die enge Zweckbindung – Vermeidung des Missbrauchs von Visa – positiv zu betrachten. Gleichwohl ist durch die Änderung des Aufenthaltsgesetzes ein sehr viel weitergehender Eingriff durch den Abgleich der Daten zu allen Personen, die an einem Visumverfahren beteiligt sind – wie z. B. Einlader, Verpflichtungsgeber und Referenzpersonen – mit der Antiterrordatei geplant.

Das weitere Gesetzgebungsverfahren (BR-Drs. 318/11) wird auch durch den Landesbeauftragten begleitet.

5.2 Gesetzentwurf zur Änderung des Gesetzes über das Ausländerzentralregister

Im IX. Tätigkeitsbericht (Nr. 6.2) erläuterte der Landesbeauftragte das Urteil des Europäischen Gerichtshofes (EuGH) vom 16. Dezember 2008 zur Unzulässigkeit gespeicherter Daten im Ausländerzentralregister (NVwZ 2009, 379) und wies darauf hin, dass aus diesem Urteil Folgerungen durch Gesetzesänderungen zu ziehen seien.

Ein Referentenentwurf eines Gesetzes zur Änderung des Gesetzes über das Ausländerzentralregister (AZR) wurde im Sommer 2010 an die Innenministerien und Senatsverwaltungen für Inneres der Länder zur Ressortabstimmung versandt.

Ziel war die Umsetzung der Grundsätze, welche im o. g. Urteil an eine Speicherung und Nutzung der Daten im AZR geknüpft sind.

In der Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, welcher sich der Landesbeauftragte anschloss, wurde darauf verwiesen, dass der Gesetzesentwurf die Vorgaben des EuGH nur unzureichend umsetze. So sieht der Referentenentwurf noch immer die Speicherung eines größeren Umfangs der Daten von Unionsbürgern vor, als es nach den Vorgaben des EuGH zulässig wäre. Auch die Übermittlung dieser Daten ausschließlich zu aufenthaltsrechtlichen Zwecken und nur an die in diesem Bereich zuständigen Behörden wird nicht gewährleistet.

Der Landesbeauftragte bat das Ministerium des Innern, ihn in seinen Bemühungen zur datenschutzgerechten Umsetzung des EuGH-Urteils zu unterstützen.

5.3 Elektronischer Aufenthaltstitel

Der Landesbeauftragte berichtet in seinen Beiträgen 6.1 und 6.2 über den neuen Personalausweis und den elektronischen Reisepass. Diese Dokumente sind mit einem Chip versehen, auf welchem elektronisch Daten, wie Fingerabdrücke und digitales Lichtbild, gespeichert werden können.

Nach der Verordnung (EG) Nr. 380/2008 des Rates vom 18. April 2008 zur Änderung der Verordnung (EG) Nr. 1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige (ABl. L 115 vom 29. April 2008, S. 1) sind auch Aufenthaltstitel künftig grundsätzlich als mit biometrischen Merkmalen versehene Dokumente auszugeben. Diese Forderung setzte die Bundesregierung mit einem Anpassungsgesetz (BGBl. 2011 I S. 610) um.

Genau wie die deutschen Ausweisdokumente wird in Zukunft der elektronische Aufenthaltstitel in Scheckkartenformat ausgegeben. Weiterhin wird ein Chip enthalten sein, auf welchem zwei Fingerabdrücke und ein digitales Lichtbild gespeichert sind. Die Speicherung der Fingerabdrücke ist hier, anders als beim elektronischen Personalausweis, nicht freiwillig, sondern durch die Verordnung (EG) Nr. 380/2008 des Rates vom 18. April 2008 vorgeschrieben.

Zusätzlich kann auf der Aufenthaltskarte auch der elektronische Identitätsnachweis wie beim neuen Personalausweis gespeichert werden.

Die neuen Dokumente werden ab dem 1. September 2011 ausgegeben. In Ausnahmefällen, z. B. zum Zweck der Verlängerung der Aufenthaltsdauer um einen Monat, können auch die herkömmlichen Klebeetiketten weiter verwandt werden.

6 Ausweis- und Melderecht

6.1 Neuer Personalausweis (nPA)

Bereits in seinem IX. Tätigkeitsbericht (Nr. 7.2) berichtete der Landesbeauftragte über die Einführung des neuen „elektronischen“ Personalausweises (nPA) zum 1. November 2010, dessen technische Voraussetzungen und der damit einhergehenden elektronischen Identifizierung (eID).

Die Abkürzung des elektronischen Personalausweises „ePA“ wurde in „nPA“ für neuer Personalausweis abgeändert.

Der Landesbeauftragte besuchte im Vorfeld verschiedene Veranstaltungen und informierte sich über die aktuelle Entwicklung zum nPA.

6.1.1 Die Feldtestphase in Sachsen-Anhalt

Aus Sachsen-Anhalt nahmen mehrere Kommunen an der Feldtestphase teil, in welcher einzelne Personalausweisbehörden den nPA und die zugehörige Technik erprobten. Ausgewählte Personalausweisbehörden wurden je nach genutzter Fachanwendung besucht. Im Gegensatz zu Städten in anderen Bundesländern gab es aus technischer Sicht keine gravierenden Schwierigkeiten. Erwartet wurden Integrationsprobleme bei der Nutzung der Software der Bundesdruckerei durch die Fachanwendungen.

Beklagt wurden vor Ort jedoch die terminlichen Vorgaben durch die Bundesdruckerei, bei denen nur der Endtermin für die Einführung (1. November 2010) feststand und die Tests und Auslieferungen von Berechtigungskarten und Test-Personalausweisen teilweise um Monate verspätet erfolgten. So war beim Informationsbesuch Mitte Oktober 2010 das Sperrmanagement noch gar nicht getestet worden und auch die Test-Personalausweise lagen in den Personalausweisbehörden noch nicht vor. Das Antragsverfahren war dessen ungeachtet erprobt worden. Damit mussten die Software-Hersteller mit unzureichenden Praxistests in den Kommunen in die Echtbetriebsphase gehen, was zu kurzfristigen Nachbesserungen und ggf. unzufriedenen Kunden hätte führen können.

6.1.2 Sichere Nutzung des nPA

Wer die neuen Möglichkeiten des nPA nutzen möchte, benötigt eine Software aus dem Internet, die sogenannte AusweisApp, und als Hardware ein Kartenlesegerät. Dieses existiert als Basislesegerät, ohne PIN-Eingabefeld, als Standardleser mit Tastenfeld und als Komfortleser mit zusätzlichem Anzeigefeld. Basisleser haben zwar ein höheres Sicherheitsniveau als z. B. Benutzername und Passwort-Abfragen, dennoch sind sie angreifbar, da ein Trojaner die Tastatur des PC auslesen könnte. Daher ist es wichtig, den PC unbedingt völlig frei von Schadsoftware jeglicher Art zu halten. Das ist in Zeiten von Windows, Internetanbindungen und gleichzeitig häufig veralteten Installationen von Betriebssystem, Webbrowser und Drittanwendungen für Normalbürger nur sehr schwer, oft gar nicht zu realisieren. Daher sollte möglichst einer der besseren Lesegerätetypen eingesetzt werden.

Im Wesentlichen wird dem Nutzer des neuen elektronischen Personalausweises auferlegt, darauf zu achten:

- Der Ausweis darf nur gegenüber Behörden, z. B. zur Identitätsfeststellung, aus der Hand gegeben werden (§ 1 Abs. 1 Satz 3 Personalausweisgesetz (PAuswG)). Es gibt ein Hinterlegungsverbot, d. h. Dritte dürfen den Ausweis nicht als Pfand nutzen. Grund ist, dass der Besitzer des Ausweises die Möglichkeit hat, Funktionen desselben zu nutzen. Damit könnten u. U. Geschäfte in fremdem Namen getätigt werden. Für Auslandsreisen empfiehlt es sich, einen Reisepass als Alternative mitzuführen. Die Politik ist gefragt, hier Regelungen und Abkommen zur Nutzung im Ausland zu schaffen.

- Der nPA-Inhaber muss Maßnahmen (§ 27 Abs. 2 PAuswG) treffen, damit niemand anderes Kenntnis von der Geheimnummer erlangt. Die PIN darf insbesondere nicht in der Nähe des nPA notiert aufbewahrt werden und diese ist ggf. unverzüglich deaktivieren zu lassen.

- Der Rechner muss sich in einem aktuellen und sicheren Zustand befinden. Insbesondere sind alle Aktualisierungen des Betriebssystems, des Webbrowsers und weiterer relevanter Software vorab einzuspielen und der Virenschutz muss sich auf einem aktuellen Stand befinden und aktiviert sein. Konkret wird sogar gefordert (§ 27 Abs. 3 PAuswG), dass der Rechner nach dem Stand der Technik als sicher anzusehen sein muss. Die technischen Systeme und Bestandteile sollen vom BSI als sicher bewertet worden sein.

Der Chip des Ausweises ist im Nahbereich per Funk auslesbar, jedoch muss dafür ein Berechtigungszertifikat vorgelegt werden. Der Benutzer muss aktiv seine PIN eingeben. Ein Angriff über die Funktechnologie ist derzeit unwahrscheinlich. Wer ganz sicher gehen will, kann den Ausweis in eine elektromagnetische Felder abschirmende Metallhülle stecken.

Berechtigungszertifikate werden für Diensteanbieter im Internet ausgegeben. Vergabestelle ist das Bundesverwaltungsamt. Dieses fordert einen Identitätsnachweis und führt eine Kontrolle der benötigten Datenfelder durch. Danach erhält der Diensteanbieter für längstens 3 Jahre das Recht, die nPA-Infrastruktur zu nutzen. Über in einem öffentlichen Verzeichnis bereitgestellte Berechtigungszertifikate kann eine Webseite oder Anwendung nachvollziehen, ob der Diensteanbieter „geprüft“ wurde und welche Datenfelder ihm sichtbar sein dürfen. Das sagt jedoch nichts über die Seriosität desselben aus. Da keine Sperrlisten existierten, werden nur kurzlebige Zertifikate mit einer Gültigkeit von 2 Tagen ausgestellt. Das bedeutet, dass ein häufiger oder permanenter Internetzugriff nötig und damit die Nutzung abseits von Webseiten ggf. erschwert wird. Nach Zurückziehen der Berechtigung kann binnen spätestens 48 Stunden der jeweilige Diensteanbieter den nPA nicht mehr ansprechen.

Bereits während der Testphase zeichnete sich ab, dass die Entscheidung, beim Nutzer hauptsächlich auf Basislesegeräte zu setzen, die Sicherheit beeinträchtigen wird. Dass diese durch die fehlende Tastatur angreifbar sind, war allen Beteiligten von vornherein klar. Entsprechend war es auch nur eine

Frage der Zeit, bis erste Demonstrations-Angriffe veröffentlicht wurden. Mittels Webseiten/JavaScript nachgebildete AusweisApp-Oberflächen – also mit Methoden des klassischen Phishings – können sehr einfach Anmeldeinformationen entführt werden. Es ist also wichtig, dass die Identität des Webseitenbetreibers vorab geklärt wird, was nur bei verschlüsselter und mittels Zertifikat abgesicherter Verbindung möglich ist. Zu achten ist auf https:// als Beginn der URL und eine farblich korrekte Markierung als Aussage zur erfolgten Zertifikatsprüfung. Das ist häufig eine grün hinterlegte Adresszeile oder ein solches Piktogramm links daneben.

6.1.3 AusweisApp

Gleich mit Beginn der Auslieferungsphase wurde ein Fehler in der zentralen Anwendung, der AusweisApp, bekannt, der es Angreifern erlaubte, beliebige Inhalte auf dem Rechner zu installieren. Beim Aktualisieren der Anwendung wurden der Server und die heruntergeladenen Daten nicht ausreichend auf ihre Authentizität hin überprüft, sodass – im Falle eines Angriffs – ein anderer Server als gültige Datenquelle akzeptiert wurde. Der Fehler hätte vermieden werden können, da das Problem in Webforen bekannt war. Durch mangelnde Transparenz bei der Entwicklung wurde auf externen Sachverstand bewusst verzichtet. Medienwirksam wurden renommierte Dritte mit der Überprüfung der Anwendung beauftragt. Diese konzentrierten sich jedoch auf andere, genau eingegrenzte Schwerpunkte. Für zukünftige, derartige Projekte wird geraten, die Entwicklung in offenen Projekten in Form von Open Source Software (OSS) durchzuführen und auf das Zusammenfügen von unterschiedlichsten Komponenten verschiedener Hersteller möglichst zu verzichten, da das zu unzureichenden Verantwortlichkeiten bei der Softwareentwicklung führt.

Die AusweisApp kommt als 49 MB (Version 1.0.3 für Windows) große Anwendung. Für ein Programm, welches im Dauerbetrieb ohne besondere Oberfläche nebenher laufen soll, ist das eher überdimensioniert. Fehler waren allein aus diesem Grund schon sehr wahrscheinlich. In der Tat stellte sich dann auch heraus, dass Drittanbieteranwendungen wie die JAVA-Laufzeitumgebung enthalten sind. Das Kopieren von Installationsarchiven von Herstellerwebseiten ist völlig inakzeptabel, da dies dazu führt, dass aktualisierte Archive nicht rechtzeitig den Weg in das eigene Programmkonglomerat schaffen. So war die JAVA RE erwartungsgemäß auch völlig veraltet und enthielt altbekannte Sicherheitslücken. Desweiteren funktioniert(e) die Installation von JAVA bspw. in alten Novell-Netzwerken nur nach Abschalten des Novell-Clients. Dazu muss man aber wissen, was alles im Hintergrund mit installiert wird und dass das Fehlschlagen der Installation an einer Unverträglichkeit von JAVA und Novell (z. B. 4.91 SP4) liegt, da keine sinnvolle Fehlermeldung oder Logdatei existiert.

Wie nicht anders zu erwarten war, sind Programme, die im Internet von Herstellerseiten kopiert und neu veröffentlicht wurden, eine Quelle für Schwierigkeiten. Zum einen aufgrund mangelhafter Dokumentation, zum anderen, weil bis heute insbesondere Microsoft Windows kein zentrales und transparentes Patch- und Update-Management für alle Anwendungen anbietet. Damit bleibt es jedem Hersteller selbst überlassen, wie er dieses realisiert und so werden viele Anwendungen zwangsläufig nicht ausreichend aktualisiert. Hinzu

kommt, dass ausführbare Dateien aus unterschiedlichsten Quellen ausgeführt werden müssen und weder automatische Downloads nur vom Hersteller, noch kostenfreie Signatur- und Prüfsummen-Checks noch eine vertrauensvolle, konfigurierbare und revisionssichere Nutzung von Administratorrechten in Windows eingebaut sind. Ein Update hat Zugriff auf die sensibelsten Rechner und Netzwerkbereiche, ohne dass klar ist, was da überhaupt mit Administratorrechten installiert wird, ob es klappen wird oder ob gar das ganze Betriebssystem hinterher sich völlig anders verhält. Leider hat Microsoft im Berichtszeitraum das Angebot zur Mitarbeit bei der datenschutzgerechten Softwareentwicklung durch den Landesbeauftragten nicht aufrecht erhalten. Statt Bibliotheken von Dritten mit zu installieren ist es ggf. hilfreich, diese einfach als Voraussetzung im Installationspaket einzutragen. So kann der Administrator diese selbst in aktueller Form beschaffen und installieren.

Die zukünftige Weiterentwicklung der AusweisApp soll laut Bundesministerium des Innern in Form eines OSS-Projekts erfolgen. Auch hier gibt es noch keine Regelungen. Das bloße Veröffentlichen von Quelltext wäre ein erster, wichtiger Schritt, jedoch sichert das nicht die Weiterentwicklung durch Dritte ab. Ein denkbarer, weiterer Schritt wäre die Registrierung eines Projekts auf einer bekannten Entwicklungs-Plattform (z. B. BerliOS, SourceForge oder Google Code) und die öffentliche Weiterentwicklung dort. Es muss eine Möglichkeit zur wesentlich schnelleren Veröffentlichung von Fehlerbehebungen gefunden werden. OSS lebt vom Mitmachen und das geht nur, wenn es für Dritte auch möglich ist, selbst Hand anzulegen und Erweiterungen einzubringen.

Behörden verfügen über eine andere Technik, um die Ausweise zu nutzen. Damit beispielsweise Passämter und Meldebehörden die Ausweise beschreiben können, müssen diese eine sogenannte EAC-Box (Extended Access Control – Sichere, zertifikatsbasierte Absicherung des erweiterten Zugriffs auf den Ausweis) verwenden. Diese ist gegen unberechtigte Zugriffe besonders gesichert, jedoch erwiesen sich die Änderungsterminals (ÄNTE) (enthalten EAC-Box) bei den ersten Probeläufen als nur sehr zeitaufwändig aktualisierbar.

6.1.4 Die qualifizierte elektronische Signatur mit dem nPA

Auf dem nPA kann ein qualifiziertes elektronisches Zertifikat zur Verwendung für elektronische Unterschriften, sogenannte Signaturen, hinterlegt werden. Dies dient dazu, den Anbietern solcher Zertifikate entgegen zu kommen, indem es ihnen ermöglicht wird, diese elektronisch z. B. über das Internet bedarfsgerecht auf den nPA nachzuladen. Es ist dem Landesbeauftragten unverständlich, warum ein solches Zertifikat nicht jedem Bürger optional und kostenfrei zur Verfügung gestellt wird. Das würde dem E-Government des Staates und auch der Wirtschaft gleichermaßen zugutekommen und sich langfristig nach Meinung des Landesbeauftragten durch Einsparungen an anderen Parallelentwicklungen ähnlicher und häufig sogar unsicherer (weil z. B. nicht offengelegter) Neu- und Eigenentwicklungen oder rechtlich nicht gleichwertiger Infrastrukturen auch rechnen.

Die freie Wirtschaft hat es durch Beharren auf zwar auch sicheren, jedoch wohl insbesondere gewinnorientiert und damit mangels Verbreitung und auf-

grund von vorwiegend kostenpflichtig ausgerichteten eigenen teuren Infrastrukturen leider nicht geschafft, elektronische Unterschriften im Alltag beim Bürger dauerhaft zu etablieren. Das Nichteingreifen des Staates durch Bereitstellung entsprechender, kostenfreier, staatlicher Zertifikate schadet der Wirtschaft in ihrer Gesamtheit, dem Staat und damit letztlich dem Bürger, der zwar die Kosten tragen darf, jedoch keine äquivalenten Leistungen oder gar zeitgemäßen Komfort bei staatlichen Stellen als Gegenleistung geboten bekommt.

Eine Liste der anerkannten Anbieter von Zertifikaten für qualifizierte elektronische Signaturen wird von der Bundesnetzagentur gepflegt und kann unter der Adresse http://dpaq.de/Zertifikate genutzt werden.

6.1.5 Zulässigkeit von Ausweiskopien

Im Zusammenhang mit der Zulässigkeit der Vervielfältigung von Personalausweisen und Reisepässen hat das Innenministerium das Rundschreiben des Bundesministeriums des Innern vom 29. März 2011 zur Kenntnis übersandt. Bisher wurde grundsätzlich die Auffassung vertreten, dass das Vervielfältigen von Pässen und Personalausweisen unzulässig sei. Da eine ausdrückliche gesetzliche Regelung fehlt, wird nunmehr die Anfertigung von Ausweiskopien im Einzelfall zugelassen. Insbesondere sei die Erstellung einer Kopie dann zulässig, wenn sie erforderlich ist. Die Kopie von Ausweisdokumenten darf ausschließlich nur zu Identifizierungszwecken verwendet werden und muss als Kopie erkennbar sein. Daten der Betroffenen, die nicht zur Aufgabenerledigung benötigt werden, sind von den Betroffenen zu schwärzen. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen. Die Kopien von Ausweisdokumenten sind unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist. Letztendlich ist eine automatisierte Speicherung der Ausweisdaten nach dem Paßgesetz und Personalausweisgesetz unzulässig. Zur Thematik der Zulässigkeit von Vervielfältigungen von Ausweisdokumenten hatte der Landesbeauftragte bereits in seinem VII. Tätigkeitsbericht (Nr. 20.4) berichtet. Danach reicht es grundsätzlich aus, dass beispielsweise zur Legitimierung der Personalausweis oder der Reisepass vorgelegt und in einem Vermerk schriftlich auf die vorgelegten Ausweisdokumente hingewiesen wird (Handzeichen Sachbearbeiter).

6.2 Elektronischer Reisepass (ePass)

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 7.1) über den elektronischen Reisepass (ePass) berichtet, Sicherheitslücken dargestellt und über die praktische Einführung in einer Kommune informiert.

Der Landesbeauftragte ließ sich nun im Rahmen seiner durchgeführten Querschnittsprüfungen in mehreren Kommunen die Umsetzung sowie die praktische Handhabung des ePasses im Echtzeitbetrieb vorführen.

Für das Antrags- und Ausgabeverfahren der Reisepässe haben die Kommunen unterschiedliche Organisationsformen gewählt. Während einige Kommunen das Bürgerbüro als Anlaufstelle für die Beantragung des Reisepasses

nutzen, haben sich andere Kommunen für die Nutzung der klassischen Meldeämter entschieden.

Je nach Größe der Kommune wurden ein oder mehrere Bestellarbeitsplätze eingerichtet. Daran ausgerichtet wurde die Behördensignaturkarte, welche von der Bundesdruckerei herausgegeben wurde, jeweils mindestens auf einen Arbeitsplatz reglementiert.

Begrüßenswert war in allen aufgesuchten Kommunen die Sicherung der Signaturkarten, Passwörter, Zertifikate und der Pässe in entsprechenden Sicherheitsschränken, die eine unzulässige Verwendung nahezu unmöglich machen.

Bei der Beantragung eines Reisepasses werden die Fingerabdrücke mittels Fingerprintscanner der Bundesdruckerei eingelesen. Die Passbehörde speichert die Fingerabdrücke der beantragenden Personen für die Dauer der Herstellung des Reisepasses, um diese bei Produktionsfehlern erneut an die Bundesdruckerei liefern zu können. Zugriff auf die Fingerabdrücke, auf die Fotos und auf die Unterschriften haben nur die zuständigen Mitarbeiterinnen und Mitarbeiter der Meldestelle bzw. des Bürgerbüros.

Die authentische Übermittlung an die Bundesdruckerei wird mittels OSCI-Transport realisiert. In der Regel werden ein- bis zweimal in der Woche bzw. am Bedarf ausgerichtet Passanträge an die Bundesdruckerei geliefert.

Sobald der Pass ausgestellt und an den Passantragsteller ausgegeben wurde, werden die Fingerabdrücke automatisch aus dem Bearbeitungsprogramm gelöscht. Dies entspricht den Regelungen des § 16 Abs. 2 PassG. Danach sind die gespeicherten Fingerabdruckdaten spätestens nach Aushändigung des Passes zu löschen.

Da die Passdaten in den Kommunen überwiegend auch auf Sicherungsmedien gespeichert und je nach Kommune zwischen einer Woche und drei Monate aufbewahrt werden, sind die Fingerabdruckdaten noch vorhanden. Die Kommunen wurden darauf aufmerksam gemacht, dass eine Überschreitung der Löschungsfristen für die biometrischen Daten im ePass-Verfahren (Löschung mit Aushändigung des Reisepasses) durch die Speicherung auf Sicherungsmedien vor allem bezüglich der Fingerabdrücke nicht zulässig ist.

Lediglich eine Kommune kam der Verpflichtung zur Löschung der Fingerabdrücke mit der Abholung des Reisepasses nach, indem hier bezüglich des ePass-Verfahrens keine Sicherungsdateien gespeichert wurden.

Der Landesbeauftragte wies in diesem Zusammenhang daraufhin, dass das Bundesamt für Sicherheit in der Informationstechnik in seiner „Handreichung Informationssicherheit für deutsche Passbehörden“ ausführt, dass für temporäre Informationen im Antragsverfahren – hier explizit die digitalen Fingerabdrücke – eine dauerhafte Speicherung unzulässig ist.

Die Fingerabdrücke können – sofern der Kunde es wünscht – bei der Passaushändigung angesehen werden. Hierfür steht ein ePass-Lesegerät der Bundesdruckerei zur Verfügung. Bei einer Überprüfung kann jedoch nur er-

kannt werden, dass auf dem Reisepass Fingerabdrücke vorhanden sind. Ob die im ePass-Leser dargestellten Fingerabdrücke tatsächlich die Fingerabdrücke der Passbewerberin bzw. des Passbewerbers sind, ist nicht überprüfbar. Dies wäre jedoch dann möglich, wenn ein tatsächlicher Abgleich mit den gespeicherten Fingerabdrücken stattfinden könnte.

Den beteiligten Kommunen wurde empfohlen, in Zusammenarbeit mit den Herstellerfirmen eine Möglichkeit des Abgleichs mit den tatsächlichen Fingerabdrücken bei Ausgabe des Passes zu suchen und in das ePass-Verfahren einzubinden. Beispielsweise könnte ein geeignetes Lesegerät mit einem entsprechenden Zugriffsberechtigungszertifikat zur Verfügung stehen, um prüfen zu können, ob die gespeicherten und die persönlichen Fingerabdrücke übereinstimmen.

6.3 Fortentwicklung Meldewesen

Im Zuge der Föderalismusreform wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt.

Im Frühjahr 2011 lag dem Landesbeauftragten der Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens vor, welcher zwischen den Landesbeauftragten für den Datenschutz und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erörtert wurde.

Begrüßenswert ist der Verzicht auf die Einrichtung eines zentralen Bundesmelderegisters, welches bereits in der Vergangenheit abgelehnt wurde.

Schwerpunkte des Entwurfes sind u. a.

- Einwilligungserklärung des Betroffenen bei Auskünften für Zwecke der Markt- oder Meinungsforschung, der Werbung oder des Adresshandels
- Vereinfachung der Anmeldungen in Krankenhäusern und in Beherbergungsstätten
- Online-Zugang öffentlicher Stellen auf bestehende Meldedatenbestände
- Wiedereinführung der Mitwirkungspflicht des Vermieters bei der Anmeldung.

Es bleibt abzuwarten, welche datenschutzrechtlichen Regelungen in dem neuen Bundesmeldegesetz Berücksichtigung finden, die auch Auswirkungen auf das Landesrecht haben werden. In diesem Zusammenhang haben die Landesbeauftragten für den Datenschutz und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine gemeinsame Stellungnahme erarbeitet und viele Details aus datenschutzrechtlicher und technischer Sicht kommentiert. Das hiesige Innenministerium wurde über die datenschutzrechtlichen Anliegen informiert. An der Wiedereinführung der Vermieternebenmeldepflicht will das Bundesinnenministerium offenbar festhalten.

6.4 Adresspooling von Melderegisterauskünften

Beim Adresspooling geht es vornehmlich darum, die Ergebnisse aus Melderegisterauskünften durch Datenverarbeiter dauerhaft zu speichern und an Dritte weiterzugegeben.

Im Jahr 2010 wandte sich die Firma RISER an den Landesbeauftragten, um dessen Rechtsauffassung zum Adresspooling von Melderegistern zu erfragen.

Nach Abstimmung mit dem Innenministerium wurde RISER mitgeteilt, dass das von RISER an alle Landesinnenministerien gerichtete Schreiben zum Adresspooling im Interesse einer zwischen Bund und Ländern abgestimmten Rückäußerung auf Vorschlag des Bundesministeriums des Innern nur von dort beantwortet werde. Die Ausführungen des Bundesministeriums zum Adresspooling allgemein sowie zu den von RISER aufgeworfenen Fragen berücksichtigen im Übrigen die dazu eingeholten Einschätzungen der Länder.

Im Ergebnis ist ein Adresspooling, das heißt das dauerhafte Speichern von Melderegisterauskünften und ihre Verwendung für einen anderen als den ursprünglichen Zweck, nicht zulässig. Diese Auffassung wird auch vom Landesbeauftragten vertreten.

Das Ministerium des Innern des Landes Sachsen-Anhalt hat schon mit Erlass vom 10. September 2008 Verfahrensregeln zur Erteilung von Melderegisterauskünften nach § 33 des Landesmeldegesetzes festgelegt.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat im Februar 2011 die RISER ID Services GmbH für ihr datensparsames und datenschutzkonformes Verfahren zum Einholen von Adressauskünften bei Meldebehörden in Europa mit dem europäischen Datenschutzsiegel EuroPriSe ausgezeichnet. Danach verzichtet RISER auf das Ansammeln eigener Datenbankbestände.

6.5 Melderegisteranfragen der Regis24 GmbH im Auftrag der Bundesagentur für Arbeit

Im Rahmen einer Länderumfrage wurde dem Landesbeauftragten bekannt, dass öffentliche Melderegisteranfragen im Namen der Bundesagentur für Arbeit (BA) durch die Firma Regis24 GmbH gestellt werden. Eine Stadt in Sachsen-Anhalt wandte sich an den Landesbeauftragten, da sie eine Melderegisteranfrage des Dienstleisters Regis24 GmbH im Namen der BA erhalten hatte.

Die BA hat die Firma Regis24 GmbH beauftragt, zum Zwecke der Einziehung von Forderungen der BA in ihrem Namen Melderegisterauskünfte über den Aufenthalt von Schuldnern einzuholen. Die BA hat die Auftragserteilung an die Firma Regis24 GmbH bestätigt. Bei der Inanspruchnahme der Firma Regis24 GmbH durch die BA ist sicherzustellen, dass die Firma Regis24 GmbH die in diesem Zusammenhang übermittelten Daten getrennt von ihrem übrigen Datenbestand zu halten hat. Dies geht aus dem Vertrag zwischen der BA und der Firma Regis24 GmbH hervor. Auch hat die BA ein umfangreiches

Prüfungsrecht mit der Firma Regis24 GmbH vereinbart, sodass der Landesbeauftragte in diesem Zusammenhang keine Bedenken gegen eine Auskunftserteilung nach § 29 Meldegesetz Sachsen-Anhalt (MG LSA) an die Firma Regis24 GmbH sieht. Eventuell bestehende Auskunfts-/Übermittlungssperren (§ 34 Abs. 4 und § 35 Abs. 2 bis 4 MG LSA) sind hierbei zu beachten.

Das Ministerium des Innern hat aufgrund der bestehenden Rechtslage von einer Information an die Meldebehörden in Sachsen-Anhalt abgesehen. Da dem nachgeordneten Bereich keine Probleme in dieser Angelegenheit bekannt geworden sind, besteht zum gegenwärtigen Zeitpunkt kein Handlungsbedarf.

7 Europäischer und Internationaler Datenschutz

Mit der Aufnahme der Grundrechte-Charta in das Europäische Vertragswerk (über Art. 6 Abs. 1 Satz 1 des Vertrages über die Europäische Union) infolge des am 1. Dezember 2009 in Kraft getretenen Lissabon-Vertrages hat auch der Datenschutz eine verbindliche Stärkung erfahren. Das betrifft vor allem Art. 7 (Recht auf Achtung des Privatlebens und der Kommunikation) und Art. 8 (Recht auf Schutz der personenbezogenen Daten) der Grundrechte-Charta.

Dieses Grundrechtspaar wirkt auch auf die Überprüfung des Europäischen Rechtsrahmens, insbesondere die Überarbeitung der Datenschutzrichtlinie von 1995, durch die Europäische Kommission ein (s. Nr. 3.1).

Parallel soll eine Novellierung der Europarats-Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten erfolgen. Dieses Übereinkommen wurde am 28. Januar 2011 30 Jahre alt und ist Pate des Europäischen Datenschutztages (s. Nr. 3.3).

7.1 Entwicklung der Sicherheitspolitik der EU – Stockholmer Programm

Mit der Entwicklung des „Stockholmer Programms“ hat die Europäische Kommission in der zweiten Hälfte des Jahres 2009 ein Konzept entworfen, das die politischen Ziele zur Weiterentwicklung des Raums der Freiheit, der Sicherheit und des Rechts für die Bürger der Union für die nächsten fünf Jahre festschreibt.

Das vom Europäischen Rat gebilligte Programm hebt zwar einerseits die Wahrung der persönlichen Freiheitsrechte und den Schutz der Privatsphäre hervor. Als Instrumente sollen zur Umsetzung Aufklärungskampagnen zum Datenschutz und die Förderung von datenschutzfreundlichen Technologien dienen. Ein umfangreicher Katalog der Europäischen Kommission enthält aber andererseits besonders eingriffsintensive Maßnahmen wie z. B. ein elektronisches Register- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in und aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb im Oktober 2009 eine Entschließung („Datenschutzdefizite in Europa

auch nach Stockholmer Programm“, **Anlage 5**) verabschiedet, in der sie Maßnahmen benennt, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen.

Der Bundesrat hat in seinem Beschluss vom 4. Juni 2010 (BR-Drs. 246/10) konkretere Vorschläge der Kommission in deren Aktionsplan kritisch bewertet. So wurde festgestellt, dass die Vorschläge teilweise den Rahmen des Stockholmer Programms überschreiten und teilweise weit hinter ihm zurückbleiben.

7.2 Neues Abkommen zu SWIFT

Bereits im VIII. Tätigkeitsbericht (Nr. 7.6) schilderte der Landesbeauftragte datenschutzrechtliche Bedenken im Zusammenhang mit dem bestehenden Abkommen zu SWIFT und der damit verbundenen Datenübermittlung an die USA.

Das Ziel aller Datenschutzbeauftragten in Europa war, die Regelungen zu datenschutzrechlichen Fragen entscheidend nachzubessern. So forderte bereits die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2009 in Berlin in einer Entschließung: „Kein Ausverkauf von europäischen Finanzdaten an die USA!“ (**Anlage 4**). Auch aus anderen Kreisen wurde Kritik zum bestehenden Abkommen laut. So rügte unter anderem die Bundesjustizministerin den fehlenden Rechtsschutz.

Die weitere Datenübermittlung im Rahmen von SWIFT an die USA wurde erst einmal gestoppt. Ein weiteres Betriebszentrum wurde in der Schweiz errichtet. Die Daten werden nun dort gespiegelt und nicht, wie bisher, in den USA.

In den USA wurde durch das amerikanische Finanzministerium nach den Terroranschlägen vom 11. September 2001 ein Programm zum Aufspüren der Finanzierung des Terrorismus (Terrorist Finance Tracking Program – TFTP) entwickelt. Für die Umsetzung dieses Programms benötigten die Amerikaner auch die Transaktionsdaten aus Europa. Somit waren auch sie am Zustandekommen eines Abkommens interessiert, das ihnen die weitere Übermittlung der benötigten Daten garantiert.

Der Bundesrat verabschiedete hierzu am 27. November 2009 (BR-Drs. 788/09) eine Entschließung, in welcher er unter anderem die verfassungsrechtlichen Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung hervorhebt, und die Bundesregierung bittet, einem Abkommen nur zuzustimmen, wenn Zweck und Voraussetzungen der Datenübermittlung klar festgelegt sind, eine Weitergabe der Daten an Drittländer ausgeschlossen und ein effektiver Rechtsschutz gewährleistet ist.

Ebenfalls am 27. November 2009 veröffentlichte der Rat der Europäischen Union (Drs. 16110/09) einen Beschluss über die Unterzeichnung eines beabsichtigten neuen Abkommens zwischen der Europäischen Union und den USA, welches am 1. Februar 2010 in Kraft treten und bis zu diesem Zeitpunkt vorläufig angewendet werden sollte. In diesem Abkommen wurden die wesentlichen Forderungen des Bundesrates, der Datenschutzbeauftragten

und vieler anderer Kritiker nicht berücksichtigt. Trotz aller Bedenken wurde das Abkommen am 30. November 2009 unterzeichnet.

Am 11. Februar 2010 hat das Europäische Parlament gegen das Abkommen gestimmt und somit die Weitergabe der Transaktionsdaten an die amerikanischen Terrorfahnder unterbrochen.

Noch im Frühjahr 2010 handelte die Kommission daraufhin ein geändertes Abkommen mit den USA aus, welches am 28. Juni 2010 unterzeichnet wurde.

Nach Zustimmung des Europäischen Parlaments ist das neue SWIFT-Abkommen am 1. August 2010 in Kraft getreten.

Eine Datenübermittlung an die USA soll nun nur noch auf Antrag erfolgen. Dabei muss das Auskunftsersuchen so eng wie möglich gefasst sein, um die zu übermittelnden Daten auf ein Minimum zu beschränken. Inlandsüberweisungen und Überweisungen innerhalb der EU sollen nicht mehr erfasst werden. Gleichzeitig mit der Anfrage an SWIFT geht eine Kopie des Ersuchens an EUROPOL, wo überprüft wird, ob die Anfrage im Rahmen des Abkommens erfolgt. Erst nach Prüfung der Rechtmäßigkeit durch EUROPOL sind die Daten zu übermitteln.

Auch Auskunfts- und Beschwerderechte wurden im neuen Abkommen geregelt. Hiernach ist der Antrag auf Auskunft an die zuständige nationale Datenschutzbehörde zu richten, welche die Anfrage dann an den Datenschutzbeauftragten des Finanzministeriums der USA weiterleitet. Von dort erfolgt dann die Meldung, ob Auskunft erteilt werden kann oder ob Daten berichtigt oder auch gelöscht worden sind. Gegen diese Entscheidung des Finanzministeriums der USA kann Rechtsmittel eingelegt werden.

Im März 2011 wurde ein Bericht bekannt, wonach EUROPOL Datenschutzverletzungen im Rahmen des Abkommens bemängelt. Die Abfragen seien zu abstrakt und allgemein. EUROPOL könne daher die geforderte datenschutzrechtliche Prüfung nicht wie vorgesehen durchführen.

Diese Meldung veranlasste die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2011, eine Entschließung zu fassen, in der auf „Gravierende Defizite bei der Umsetzung des SWFT-Abkommens - dringender Handlungsbedarf auf nationaler und internationaler Ebene“ (**Anlage 21**) hingewiesen wurde.

7.3 Datenschutzabkommen zwischen der EU und den Vereinigten Staaten von Amerika

Bereits im Jahr 2009 hat das Europäische Parlament in einer Entschließung ein Abkommen zwischen der EU und den Vereinigten Staaten gefordert, das einen ausreichenden Schutz der bürgerlichen Freiheiten und der personenbezogenen Daten bei der Übermittlung von Daten und Informationen zu Strafverfolgungszwecken gewährleistet. Dieses Abkommen soll in Zukunft die Grundlage für alle Datenübermittlungen an die Vereinigten Staaten von Amerika zu Strafverfolgungszwecken bilden.

Im Sommer 2010 hat die Europäische Kommission einen ersten Entwurf eines neuen Datenschutz-Rahmenabkommens vorgelegt. Der Bundesrat begrüßt mit Beschluss vom 26. November 2010 (BR-Drs. 741/10) die Bemühungen der Kommission. Dabei betont er die Bedeutung, die dem Recht auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten zukommt.

Die europäischen Datenschutzbeauftragten fordern in diesem Zusammenhang unter anderem, dass ein solches Abkommen Standards enthält, welche nicht nur für zukünftig abzuschließende Abkommen gelten, sondern auch für bereits bestehende Abkommen umgesetzt werden. Weiterhin muss gewährleistet werden, dass europäische Bürger und Bürgerinnen ihre Datenschutzrechte in den Vereinigten Staaten durchsetzen können. Weitere Grundanforderungen sind die Beachtung der Unvereinbarkeit einer unverhältnismäßig langen anlasslosen Speicherdauer über viele Jahre mit dem europäischen Datenschutzrecht sowie die Benennung einer unabhängigen Kontrollbehörde.

Das bilaterale Abkommen zwischen Deutschland und den USA wurde trotz Bedenken u. a. des Bundesrates (BR-Drs. 637/09 (Beschluss) vom 10. Juli 2009; vgl. auch IX. Tätigkeitsbericht, Nr. 8.1) vom Bundestag verabschiedet (BGBl. II 2009 S. 1010 und BGBl. I 2009 S. 2998).

7.4 Verwendung von Flugpassagierdaten und Körperscannern

Seit vielen Jahren beobachtet der Landesbeauftragte mit Besorgnis die zunehmende Datenerfassung und -speicherung im Zusammenhang mit Flugreisen (vgl. VIII. Tätigkeitsbericht, Nr. 7.5 und IX. Tätigkeitsbericht, Nrn. 8.3 und 8.4).

Diese Thematik war auch in diesem Berichtszeitraum von unveränderter Aktualität. So legte die Europäische Kommission Anfang 2011 einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen bei europäischen Flügen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Ratsdok. 6007/11) vor.

Die Datenschutzbeauftragten des Bundes und der Länder kritisierten diesen Vorschlag in einer Entschließung der 81. Konferenz im März 2011 „Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!“ (**Anlage 22**) dahingehend, dass ein solches Zusammenspiel von Vorratsdatenspeicherung und Rasterung von Passagierdaten weder mit der EU-Grundrechte-Charta noch mit dem verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung vereinbar sei. Insbesondere im Hinblick auf die jüngste Rechtsprechung des Bundesverfassungsgerichts in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsdaten (NJW 2010, 833) wird angemahnt, dass die Bundesrepublik sich auch auf europäischer und internationaler Ebene dafür einzusetzen hat, dass die Bürgerinnen und Bürger der Bundesrepublik nicht total erfasst und registriert werden dürfen.

Auch der Bundesrat hat mit Beschluss vom 18. März 2011 (BR-Drs. 73/11) kritisiert, dass der neue Entwurf den bereits im Februar 2008 gegen den damaligen Richtlinienentwurf geäußerten Bedenken nicht in hinreichendem Maße nachkommt. Er betont, dass bei der Verfolgung des Ziels der Bekämpfung von Terrorismus und organisierter bzw. schwerer Kriminalität das Verhältnis zwischen der Wahrung der Freiheitsrechte und dem Schutz der öffentlichen Sicherheit in ein angemessenes Gleichgewicht zu bringen ist. Für die Erlangung dieses Ziels ist ein Höchstmaß an Datenschutz zu gewährleisten. In dieser Frage bestehen jedoch gegen den vorliegenden Richtlinienentwurf erhebliche Bedenken.

Weiterhin stellt der Bundesrat in seiner Stellungnahme klar, dass die Speicherung der Passenger Name Record (PNR) Daten ohne Anlass, also ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, einen besonders schweren Eingriff in die informationelle Selbstbestimmung und das Recht auf Achtung des Privatlebens darstellt. Ein solcher Eingriff kann nur dann zulässig sein, wenn im Hinblick auf das Ziel ein besonderes Bedürfnis besteht und der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Ein solcher Nachweis wurde nach Auffassung des Bundesrates auch mit dem vorgelegten Vorschlag einer Richtlinie nicht erbracht.
Die Justizministerkonferenz schloss sich dieser Kritik im Mai 2011 an.

Aber nicht nur die Speicherung der PNR stieß bei den Datenschutzbeauftragten auf Kritik, auch die Erprobung im Einsatz und die damit im Zusammenhang stehenden Probleme der Körperscanner auf deutschen Flughäfen fanden Beachtung. Hierzu haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung der 79. Konferenz im März 2010 „Körperscanner – viele offene Fragen“ (**Anlage 12**) gefordert, dass die Geräte auch einen nennenswerten Sicherheitsgewinn erzielen, beispielsweise indem sie auch Materialien mit geringer Dichte, wie etwa pulverförmige Substanzen, nachweisen, die Speicherung der beim Einsatz des Körperscanners erhobenen Daten ausgeschlossen wird, sowie die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzt werden.

Auch die Europäische Datenschutzkonferenz hat sich im April 2010 („Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen“, **Anlage 35**) für die Einhaltung der grundlegenden Datenschutzbestimmungen ausgesprochen.

Die Tests der Körperscanner am Flughafen Hamburg ergaben technische Mängel bzw. zu viele Fehlalarme. Die Nutzung der Körperscanner war auf freiwilliger Basis möglich. Das Bundesinnenministerium dürfte das Vorhaben absagen.

Der Landesbeauftragte wird in beiden Fällen die weitere Entwicklung kritisch begleiten. Für die Körperscanner könnte eine europäische Regelung kommen.

7.5 Europäische Datenschutzkonferenzen

Die Europäische Konferenz der Datenschutzbeauftragten einigte sich im April 2009 auf eine Entschließung, in welcher die Notwendigkeit einheitlicher Datenschutzstandards bei bilateralen und multilateralen Abkommen im Bereich der polizeilichen und justiziellen Zusammenarbeit bekräftigt wurde (Entschließung der Frühjahrskonferenz 2009 der Europäischen Datenschutzbeauftragten zu bilateralen und multilateralen Abkommen zwischen europäischen Staaten und Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, **Anlage 33**). Weiterhin wurde eine Erklärung verabschiedet, welche die Notwendigkeit hoher Datenschutzstandards auf der Grundlage umfassender Gesetzgebung des Datenschutzes in Europa bekräftigte („Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa“, **Anlage 32**).

Bei der Europäischen Konferenz der Datenschutzbeauftragten im April 2010 lag der Schwerpunkt der Beratungen wiederum in der Verabschiedung einer Entschließung zu Anforderungen an ein geplantes Abkommen über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit (Entschließung der Frühjahrskonferenz 2010 der Europäischen Datenschutzbeauftragten zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, **Anlage 34**) sowie zum Einsatz von Körperscannern an Flughäfen (Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen, **Anlage 35**).

Auf der Europäischen Datenschutzkonferenz in Brüssel im April 2011 wurde eine Entschließung zum Rechtsrahmen für den Datenschutz gefasst (Entschließung über die Notwendigkeit eines umfassenden Rechtsrahmens für den Datenschutz, **Anlage 36**).

7.6 Internationale Konferenzen der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Im Mittelpunkt der 31. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im November 2009 stand die Forderung nach globalen Datenschutzstandards für eine globale Welt mittels einer Entschließung („Internationale Standards zum Schutz der Privatsphäre“, **Anlage 37**). Man erarbeitete weiter einen gemeinsamen Vorschlag zur Erstellung internationaler Standards; u. a. wurden grundlegende Prinzipien, die Notwendigkeit der Rechtfertigung der Verarbeitung und die Rechte der Betroffenen formuliert.

Die 32. Internationale Datenschutzkonferenz im Oktober 2010 diskutierte anhand der sozialen Netzwerke über die unterschiedlichen Anforderungen der verschiedenen Generationen an den Datenschutz. Dabei wurden die aktuellen Herausforderungen hervorgehoben, die aufgrund der Entwicklung immer neuer Technologien an den Datenschutz gestellt werden. Bereits bei der Entwicklung von Entwürfen solcher informationstechnischen Systeme sollten die Datenschutzanforderungen frühzeitig Berücksichtigung finden.

8 Finanzwesen

8.1 Auskunftsrecht für Betroffene im Steuerverfahren – Teil II

In seinem IX. Tätigkeitsbericht (Nr. 9.1) verwies der Landesbeauftragte auf eine Verwaltungsanweisung des Bundesministeriums der Finanzen, in welcher der Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren von einem „berechtigten Interesse“ abhängig gemacht wird. Diese Verfahrensweise entspricht nach Auffassung des Landesbeauftragten nicht der Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 10. März 2008, 1 BvR 2388/03, NJW 2008, 2099).

Auch ist die Landesregierung der Meinung, dass der Beschluss nur für „Datensammlungen, bei denen die Daten entweder ohne Mitwirkung des Betroffenen erhoben werden oder deren Speicherung von dem ursprünglichen Erhebungszweck gelöst wird“, gilt (Stellungnahme zum IX. Tätigkeitsbericht des Landesbeauftragten, LT-Drs. 5/2385).

Allerdings ist, mangels spezialgesetzlicher Regelung in der Abgabenordnung, grundsätzlich die allgemeine Regelung zum Auskunftsrecht im § 19 BDSG – und somit auch § 15 DSG-LSA – anwendbar. Wenn bereits ein Auskunftsanspruch nach § 19 BDSG bzw. § 15 DSG-LSA für diese sensibleren, unter Umgehung des Grundsatzes der Erhebung beim Betroffenen gewonnenen Daten bejaht wird, ist erst recht von einem Auskunftsanspruch bezüglich der Daten im Besteuerungsverfahren bei den Finanzämtern auszugehen.

Die Datenschutzbeauftragten des Bundes und der Länder verstärkten im zurückliegenden Berichtszeitraum ihre Bemühungen, eine einheitliche Regelung in der Abgabenordnung zu schaffen, die dem Beschluss des Bundesverfassungsgerichts vom 10. März 2008 und den allgemeinen datenschutzrechtlichen Regelungen zum Auskunftsrecht gerecht wird.

Die Landesregierung wies in ihrer Stellungnahme zum I. Tätigkeitsbericht des Landesbeauftragten für die Informationsfreiheit vom 10. Dezember 2010 (LT-Drs. 6/131) auf die zurzeit stattfindende Erörterung eines Entwurfs eines Auskunftsanspruchs in der Abgabenordnung und konkret darauf hin, dass an dem Erfordernis der Darlegung eines Informationsinteresses nicht mehr festgehalten wird. Eine klarstellende Regelung soll der Finanzbehörde die Möglichkeit geben, im Einzelfall die Darlegung des Informationsinteresses zu fordern.

Eine solche Formulierung in der Abgabenordnung wäre zwar bereits eine Verbesserung zur Verwaltungsanweisung des Bundesministeriums der Finanzen, jedoch stände sie immer noch hinter der voraussetzungslosen Gewährung des Auskunftsanspruchs nach § 19 BDSG bzw. § 15 DSG-LSA zurück.

Ein in diesem Sinne überarbeiteter Entwurf einer gesetzlichen Regelung liegt bis heute nicht vor.

8.2 Ablösung der Lohnsteuerkarte – ELStAM

Im IX. Tätigkeitsbericht (Nr. 9.4) berichtete der Landesbeauftragte über die Gesetzgebung zum Wegfall der Lohnsteuerkarte zum Jahr 2011.

Wie bereits dargelegt, wurde zu diesem Zweck beim Bundeszentralamt für Steuern eine Datenbank geschaffen, die Daten wie Religionszugehörigkeit, Familienstand und Angaben zu Angehörigen einer Person, welche bisher nur in den einzelnen Meldebehörden gespeichert waren, in einer bundesweiten Datenbank mit weiteren steuerlich relevanten Daten zusammenfasst, die sogenannten elektronischen Lohnsteuerabzugsmerkmale (ELStAM). Da die Daten in Zukunft für den Abruf durch die Arbeitgeber bereitstehen, kann auf die bisherige Lohnsteuerkarte verzichtet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fasste hierzu am 24. Juni 2010 die Entschließung „Erweiterung der Steuerdatenbank enthält große Risiken“ (**Anlage 14**), da die Befürchtung bestand, dass z. B. Arbeitgeber Daten unberechtigt abrufen könnten.

Hierzu hat der Gesetzgeber inzwischen Regelungen getroffen. So kann aufgrund des neu eingeführten § 52b Abs. 8 Einkommensteuergesetz jede Arbeitnehmerin und jeder Arbeitnehmer die Bereitstellung der ELStAM für bestimmte Arbeitgeber freigeben oder sperren lassen.

Bei der Verfahrensentwicklung kam es zu Verzögerungen, sodass der geplante Beginn der Abrufe der ELStAM auf das Jahr 2012 verschoben wurde. So lag z. B. auch das Sicherheitskonzept für das ELStAM-Abrufverfahren noch nicht vor. Wenn dieses erstellt ist, wird der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit Unterstützung der Landesbeauftragten eine Prüfung durchführen. Für das Jahr 2011 wurde eine Regelung vereinbart, die es ermöglichte, für die Steuerabführung die vorhandenen Daten des Jahres 2010 weiter zu nutzen.

8.3 Evaluierung des „anderen sicheren Verfahrens“ der ElsterOnline-Anmeldung

Im IX. Tätigkeitsbericht (Nr. 9.7) thematisierte der Landesbeauftragte die Risiken der unsicheren Authentifizierung bei der ElsterOnline-Anmeldung. Dabei wies der Landesbeauftragte auch darauf hin, dass es keine gesetzliche Definition gebe, die die Anforderungen an ein „anderes sicheres Verfahren“ klarstellt und dass eine gesetzlich vorgeschriebene Pflicht zur Evaluierung bestehe.

Im Oktober 2010 wurde der Landesbeauftragte durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von einer Besprechung mit dem Bundesministerium der Finanzen zum Evaluierungsbericht des „anderen sicheren Verfahrens“ nach § 87a Abs. 6 AO unterrichtet.

Bereits im Vorfeld hatten sich die Datenschutzbeauftragten des Bundes und der Länder auf einen Standpunkt geeinigt, welche Aspekte in einem Evaluierungsbericht zwingend zu berücksichtigen wären. Dabei stellten die Datenschutzbeauftragten klar, dass der Maßstab, an welchem das „andere sichere

Verfahren“ zu messen sei, nur die derzeit gültige rechtliche Grundlage sein kann, also die Qualifizierte elektronische Signatur (QES).

Diese und weitere durch die Datenschutzbeauftragten vorgebrachten Argumente wurden zwar durch das Bundesministerium der Finanzen zur Kenntnis genommen, doch letztlich nicht im Evaluierungsbericht berücksichtigt. Dies wurde mit der Formulierung aus dem Gesetz heraus begründet, wonach gemäß § 87a Abs. 6 Satz 3 AO die Verwendung eines anderen sicheren Verfahrens zu evaluieren ist. Eine Beurteilung möglicher Alternativen sei nicht verlangt worden. Das Bundesministerium der Finanzen vertritt die Ansicht, dass somit nicht die Schutzmöglichkeiten, die die QES bietet, zu betrachten seien, sondern nur, ob es bei der Benutzung des „anderen sicheren Verfahrens“ zu sicherheitsrelevanten Problemen gekommen sei.

Ziel der Einführung eines „anderen sicheren Verfahrens“ ist es, die elektronische Übermittlung steuerlich relevanter Daten zu fördern. Hierzu muss das Verfahren so anwenderfreundlich wie möglich gestaltet werden. Dies wird erreicht, indem die ursprünglichen hohen Schutzanforderungen an eine elektronische Übermittlung der Daten durch eine QES heruntergefahren werden.

Das „andere sichere Verfahren“ muss gewährleisten, dass die übermittelten Daten einem Absender zugeordnet werden können (Authentizität), nicht unbemerkt verändert werden können (Integrität) und dass das Steuergeheimnis gewahrt wird.

Bereits die eindeutige Zuordnung einer mittels „anderem sicheren Verfahren“ elektronisch übermittelten Erklärung zu einem bestimmten Absender kann laut Evaluierungsbericht nicht sichergestellt werden. Jedoch eine Zuordnung der übermittelten Daten zu einem bestimmten Nutzerkonto ist möglich und dieses wird einer Steuernummer zugeordnet. Somit kann über die Steuernummer der Inhaber des Nutzerkontos identifiziert werden.

Wenn jedoch der Übermittler der Daten nicht der Steuerpflichtige ist, sondern z. B. ein Steuerberater, authentifiziert sich der Datenübermittler gegenüber der Finanzverwaltung. In diesem Fall geht erst einmal die Finanzverwaltung davon aus, dass der Steuerberater ermächtigt war, diese Steuererklärung für den betreffenden Steuerpflichtigen zu übermitteln.

Die Feststellung der Authentizität der Erklärung bleibt also trotz Zuordnung der Daten zu einem Steuerpflichtigen problematisch. Im Evaluierungsbericht wird dazu darauf verwiesen, dass selbst bei der herkömmlichen Steuererklärung auf Papier nicht ausgeschlossen werden konnte, dass die Unterschrift gefälscht wurde.

Weiterhin räumte das Bundesministerium der Finanzen ein, dass in den zurückliegenden Jahren Einzelfälle bekannt geworden sind, in denen fehlerhafte Datenübermittlungen stattgefunden hatten. Das Bundesministerium der Finanzen ordnete diese Datenübermittlungen jedoch als Testübermittlungen ein, in welchen vergessen wurde, den für solche Übermittlungen vorgesehenen Testmerker zu setzen, oder um bewusste Fehlübermittlungen, um auf Missbrauchsmöglichkeiten in diesem Verfahren aufmerksam zu machen. Es

wird betont, dass es in keinem Fall zu Schäden oder strafrechtlichen Ermittlungen kam.

Somit wird durch den Evaluierungsbericht das „andere sichere Verfahren“ zur elektronischen Übermittlung steuerrelevanter Daten als Verfahren bewertet, welches sich in der Praxis bewährt hat.

Als Folge der Evaluierung soll nun gemäß Entwurf des Steuervereinfachungsgesetzes 2011 (BT-Drs. 17/5125) die Befristung der Möglichkeit der Nutzung des „anderen sicheren Verfahrens“ bis 31. Dezember 2011 gestrichen werden. Somit wäre die Nutzung des „anderen sicheren Verfahrens“ auf Dauer möglich.

9 Forschung

9.1 Allgemeines

Der Landesbeauftragte wurde in diesem Berichtszeitraum bei 17 neuen Forschungsprojekten, hauptsächlich im Bildungs- und Gesundheitsbereich, beteiligt. Darüber hinaus waren einige sich in bestimmten Zeitabständen wiederholende Projekte zu begleiten. Dazu waren umfangreiche Unterlagen (Fragebögen, Informationsschreiben und Einwilligungserklärungen) zu prüfen. Die forschenden Einrichtungen wurden z. T. ausführlich aus datenschutzrechtlicher Sicht beraten. Die Hinweise und Empfehlungen wurden größtenteils in den Projekten berücksichtigt. Es handelte sich dabei im Wesentlichen um Empfehlungen, die eine informierte Einwilligung gewährleisten sollten, z. B. durch eine genauere Beschreibung des Verfahrens sowie der beabsichtigten weiteren Datenverwendung und eine detailliertere Angabe des Zeitpunktes der Datenlöschung.

10 Gefahrenabwehr

10.1 Kontrolle des Hunderegisters

In seinem IX. Tätigkeitsbericht (Nr. 11.1) hat der Landesbeauftragte über das Gesetzgebungsverfahren für das Gesetz zur Vorsorge gegen die von Hunden ausgehenden Gefahren berichtet. Das Gesetz trat Anfang 2009 in Kraft. Das auf Grundlage dieses Gesetzes errichtete zentrale Register (Hunderegister) wird beim Landesverwaltungsamt betrieben. Um sich ein Bild von der praktischen Umsetzung der Vorschriften über das Hunderegister zu machen, hat der Landesbeauftragte einen Informations- und Kontrollbesuch beim Landesverwaltungsamt durchgeführt.

Anlässlich des Besuchs wurden dem Landesbeauftragten die Möglichkeiten, die das Hunderegister dem Landesverwaltungsamt und auch den Gemeinden bietet, vorgestellt. Das Landesverwaltungsamt ist als Aufsichtsbehörde nunmehr in der Lage, sozusagen auf Knopfdruck, statistische Erhebungen für das gesamte Land durchzuführen. Auch die Gemeinden können das Register nach bestimmten Suchkriterien durchsuchen.

Im Ergebnis seines Besuches musste der Landesbeauftragte feststellen, dass ein Datum in das Hunderegister aufgenommen wurde, welches nach den Vorschriften des Gesetzes für die Erfassung im Register nicht vorgese-

hen ist und dass bei zumindest einer Gemeinde die Eintragungen wenig plausibel erschienen.

Der Landesbeauftragte hat das Landesverwaltungsamt daraufhin gebeten, das Hunderegister um das zusätzliche Datum zu bereinigen. Nach einigem Schriftverkehr mit dem Landesverwaltungsamt und dem Ministerium des Innern des Landes Sachsen-Anhalt wurde das streitige Datum im Rahmen einer Softwareüberarbeitung aus dem Hunderegister entfernt und damit ein rechtmäßiger Zustand hergestellt. Entsprechendes teilte das Landesverwaltungsamt im Februar 2011 mit.

Unter dem Eindruck der Feststellungen hat der Landesbeauftragte auch die „Festlegungen für ein automatisiertes Verfahren für das Verfahrensverzeichnis“ einer erneuten Überprüfung unterzogen. Auf Anregung des Landesbeauftragten hat das Landesverwaltungsamt eine entsprechende Überarbeitung vorgenommen und im Februar 2011 ein überarbeitetes Verfahrensverzeichnis vorgelegt.

Um seinen Erkenntnisstand zum Hunderegister zu vervollständigen und zur Klärung festgestellter wenig plausibler Eintragungen, unterzog der Landesbeauftragte im März 2011 auch eine Kommune einer Kontrolle. Im Ergebnis konnte der Landesbeauftragte feststellen, dass datenschutzrechtlichen Belangen im Rahmen der Nutzung des zentralen Hunderegisters grundsätzlich Rechnung getragen wird. Aufgefallen sind dem Landebeauftragten allerdings zunächst unerklärliche Zahlen im Rahmen der statistischen Auswertung. Nach den Angaben im zentralen Hunderegister hat die überprüfte Kommune annähernd doppelt so viele Hundehalter wie Hunde registriert. Die zuständigen Mitarbeiter erklärten jedoch, zu jedem Hund nur jeweils einen Hundehalter registriert zu haben. Weil nicht ausgeschlossen werden konnte, dass die Angaben zu den Hundehaltern auch technisch bedingt fehlerhaft sind, wurde das Landesverwaltungsamt gebeten, die Ursachen für dieses Problem gemeinsam mit der Kommune aufzuklären.

10.2 Landesversammlungsgesetz

Wie der Landesbeauftragte in seinem IX. Tätigkeitsbericht (Nr. 11.2) geschildert hat, wurde der Vorschlag zum Erlass eines auf das Versammlungsgesetz des Bundes verweisenden Gesetzes im Rahmen der parlamentarischen Beratungen verworfen und ein Vollgesetzentwurf zur Grundlage der Beratungen gemacht. Diese Entwicklung begrüßte der Landesbeauftragte ausdrücklich.

Am 3. Dezember 2009 hat der Landtag von Sachsen-Anhalt das Gesetz des Landes Sachsen-Anhalt über Versammlungen und Aufzüge (GVBl. LSA S. 558) beschlossen. In Kraft getreten ist das Gesetz am 12. Dezember 2009. Die in § 18 des Gesetzes getroffene Regelung zu Bild- und Tonaufzeichnungen begegnet derzeit keinen datenschutzrechtlichen Bedenken, weil sie sich an den Vorgaben des Bundesverfassungsgerichtes orientiert.

Über diese landesrechtlichen Bezüge hinaus soll an dieser Stelle auch auf die Entscheidung des Bundesverfassungsgerichtes vom 22. Februar 2011 (NJW 2011, 1201) hingewiesen werden, die die Versammlungsfreiheit da-

durch stärkt, dass sie für die öffentlich zugänglichen Bereiche eines Flughafens, der sich überwiegend in öffentlicher Hand befindet, die gleiche Grundrechtsbindung wie für im Alleineigentum des Staates stehende öffentliche Unternehmen feststellt. Anlass für die Entscheidung des Bundesverfassungsgerichtes bildete der Streit zwischen dem Flughafen Frankfurt, der sich zu 52% in öffentlicher Hand befindet, und der Beschwerdeführerin über ein durch den Flughafen Frankfurt erlassenes generelles Demonstrationsverbot. Das Gericht betonte nun, dass der Flughafen Frankfurt gegenüber der Beschwerdeführerin unmittelbar an die Grundrechte gebunden ist. Diese Grundrechtsbindung umfasst nicht nur das Grundrecht auf Versammlungsfreiheit, sondern alle Grundrechte – insbesondere auch das Grundrecht auf freie Meinungsäußerung.

10.3 Änderung des Spielbankgesetzes

Wie der Landesbeauftragte in seinem IX. Tätigkeitsbericht (Nr. 11.3) ausführlich dargestellt hat, hat die Landesregierung im Jahr 2008 den Entwurf eines neuen Spielbankgesetzes für das Land Sachsen-Anhalt erarbeitet. Der Landesbeauftragte war in diesen Prozess mit eingebunden, seine Bedenken wurden allerdings nicht umfassend berücksichtigt. Der im Februar 2009 eingebrachte Gesetzentwurf (LT-Drs. 5/1785) entsprach in verschiedener Hinsicht nicht den datenschutzrechtlichen Vorstellungen des Landesbeauftragten.

Im Rahmen der Ausschussberatungen des Landtages konnte zumindest noch eine deutliche Verbesserung erreicht werden. Von den drei zum Gesetzentwurf noch verbliebenen Hauptbedenken des Landesbeauftragten konnte eines ausgeräumt werden.

Soweit es die Regelungen zur Spielbankaufsicht in § 20 Abs. 3 des Gesetzentwurfes betrifft, konnte erreicht werden, dass das Landeskriminalamt zur Unterstützung der Spielbankaufsicht nicht mehr alle Erkenntnisse zu Straftaten und Gefahrenlagen ohne Einschränkung sammeln und auswerten darf. Vielmehr muss es sich bei den zu sammelnden und auszuwertenden Erkenntnissen um solche handeln, die beim Betrieb von Spielbanken auftreten.

Keine Verbesserung im datenschutzrechtlichen Sinne konnte bei den Regelungen zur Videoüberwachung in § 8 und denen zum Spielangebot in § 9 erzielt werden. Hier hält der Landesbeauftragte an seinen Bedenken fest und verweist auf die Ausführungen in seinem IX. Tätigkeitsbericht.

Neben den datenschutzrechtlichen Verbesserungen und den nicht umgesetzten Empfehlungen des Landesbeauftragten musste der Landesbeauftragte aber auch Verschlechterungen feststellen. So sind nach § 9 Abs. 3 jetzt alle Betriebsdaten der Glücksspielautomaten laufend zu erfassen und zu dokumentieren. Im ursprünglichen Gesetzentwurf der Landesregierung beschränkte sich die Erfassung und Dokumentation noch auf alle wesentlichen Betriebsdaten. Darüber hinaus wurde in § 20 Abs. 5 eine Verpflichtung für Finanzämter geschaffen, das für Spielbankaufsicht zuständige Ministerium über die für die Wahrnehmung der Aufsichtspflichten bedeutenden Kenntnisse zu unterrichten. Alle sonstigen Landesfinanzbehörden sind zur Unterrichtung berechtigt. Im ursprünglichen Gesetzentwurf der Landesregierung wa-

ren alle Finanzbehörden – also auch die Finanzämter – lediglich berechtigt, Kenntnisse zu offenbaren.

Das Spielbankgesetz des Landes Sachsen-Anhalt wurde vom Landtag von Sachsen-Anhalt in seiner Sitzung am 16. Dezember 2009 beschlossen und am 21. Dezember 2009 im Gesetz- und Verordnungsblatt (GVBl. LSA S. 691) verkündet.

Eine Forderung des Landesbeauftragten zum Gesetzentwurf hat die Landesregierung mit der Verordnung über die Spielordnung in öffentlichen Spielbanken vom 22. Dezember 2009 (SpielO-VO, GVBl. LSA S. 759) umgesetzt. In § 2 Abs. 2 SpielO-VO wurde eine Regelung aufgenommen, wonach auf den Eintrittskarten deutlich sichtbar und gut lesbar auf den Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen in Spielbanken hingewiesen werden muss.

10.4 Abrufverfahren bei der Waffenbehörde

Bereits in seinem IX. Tätigkeitsbericht (Nr. 11.4) hat der Landesbeauftragte dargestellt, dass ein Landkreis ein automatisiertes Abrufverfahren bei seiner unteren Waffenbehörde zugunsten eines Polizeireviers eingerichtet hatte. Im Berichtszeitraum hat der Landesbeauftragte das Verfahren nunmehr vor Ort in Augenschein genommen.

Im Ergebnis des Informations- und Kontrollbesuches musste festgestellt werden, dass die Protokolldaten nicht, wie in der Vereinbarung zwischen dem Landkreis und der Polizei festgelegt, nach einem Jahr gelöscht wurden. Darüber hinaus wurde das Verfahren zur Passwortvergabe und zur Aufbewahrung von Passworten hinterfragt. Der Landkreis wurde durch den Landesbeauftragten auf diese datenschutzrechtlichen Defizite hingewiesen und aufgefordert, diese abzustellen.

10.5 Anforderungen an den Informantenschutz

Im Umweltrecht handelt es sich um eine häufige Konstellation, dass eine Behörde erst aufgrund von Informationen Dritter ein Verwaltungsverfahren einleitet, um festzustellen, ob von einem Betrieb Belästigungen, Gefahren oder Störungen ausgehen. Meistens handelt es sich bei den Informanten um Nachbarn oder Anwohner, die sich bei der Behörde über Belästigungen beschwert haben. Nimmt der betroffene Betrieb in dem Verwaltungsverfahren sein Recht auf Akteneinsicht in Anspruch, stellt sich für die Behörde die Frage, ob sie ihm im Rahmen der Akteneinsicht auch die Namen des oder der Informanten preisgeben muss.

In einem von dem Landesbeauftragten zu prüfenden Fall hat dies ein Umweltamt eines Landkreises bejaht, weil es sich zu einer unbeschränkten Gewährung der Akteneinsicht verpflichtet glaubte. Diese Rechtsauffassung lässt sich mit der höchstrichterlichen Rechtsprechung zum Informantenschutz jedoch nicht vereinbaren. Ihr zufolge ist die Entscheidung über die Preisgabe des Namens eines Behördeninformanten im Wege der Akteneinsicht anhand einer Güterabwägung zwischen dem Interesse an der Geheimhaltung des Informanten und dem Auskunftsinteresse des Betroffenen zu treffen (BVerwG

NJW 2004, 1543 f.; BFH NJW 2007, 1311 f; VerfGH Rh-Pfalz NJW 1999, 2264 f.). Die Rechtsprechung kommt dabei zu dem Ergebnis, dass dem Interesse an der Geheimhaltung des Behördeninformanten regelmäßig ein höheres Gewicht gegenüber dem Informationsinteresse des Akteneinsichtsbegehrenden zukommt, sofern keine Anhaltspunkte dafür vorliegen, dass der Informant wider besseres Wissen oder leichtfertig falsche Behauptungen aufgestellt hat (vgl. die o. g. Rechtsprechung, a. a. O). Angaben über die Identität eines Behördeninformanten gehören daher grundsätzlich zu den ihrem Wesen nach geheimzuhaltenden Vorgängen i. S. d. § 1 Verwaltungsverfahrensgesetz Sachsen-Anhalt i. V. m. § 29 Abs. 2 Verwaltungsverfahrensgesetz des Bundes.

Der Vorrang des Schutzes eines Informanten lässt sich zum einen mit dem überwiegenden öffentlichen Interesse an der Funktionsfähigkeit von Behörden begründen. Diese sind zu ihrer Aufgabenerfüllung auf Informationen aus der Bevölkerung angewiesen, die sie nur erhalten, wenn die Vertraulichkeit gewährleistet ist. Ein Überwiegen des Informantenschutzes ergibt sich zum anderen aus dem berechtigten Interesse des Informanten, vor Nachteilen bewahrt zu werden, die er befürchten müsste, sollte der Beteiligte von seiner Tätigkeit erfahren. Aus diesem Grund setzt der Schutz des Informanten auch nicht voraus, dass dieser die Wahrung seiner Anonymität ausdrücklich verlangt hat, sondern es reicht aus, dass er nach den Umständen mit ihr rechnen konnte (VerfGH Rh-Pfalz NJW 1999, 2264/2265). Ebenso entfällt nach der Rechtsprechung der Informantenschutz nicht schon dann, wenn die der Behörde mitgeteilten Informationen letztlich nicht bewiesen werden konnten oder sich gar als unrichtig erwiesen haben, denn die Behörden können die für ihre Aufgabenerfüllung unentbehrlichen Informationen Dritter nur erwarten, wenn nicht schon jede geringe Nachlässigkeit des Informanten zu seiner Preisgabe führt (BVerwG NJW 1992, 451; VerfGH Rh-Pfalz NJW 1999, 2264/2265).

Inhaltlich verlangt der Informantenschutz in der Regel nur, dass die Identität des Informanten geheim gehalten wird; Akteneinsicht darf daher allein in den insoweit anonymisierten Vorgang gewährt werden (BayVGH NVwZ 1990, 775/778). Sollten sich aus den anonymisierten Aktenteilen dennoch Rückschlüsse auf die Person des Informanten ergeben, muss dies zur Verteidigung der Rechte des Einsichtsbegehrenden grundsätzlich hingenommen werden (vgl. BayVGH NVwZ, a. a. O).

11 Geoinformation und Vermessung

11.1 Geoinformationen

In seinem IX. Tätigkeitsbericht (Nr. 4.9) hatte der Landesbeauftragte über die Erarbeitung eines Gesetzes zum Aufbau einer Geodateninfrastruktur in Sachsen-Anhalt (GDI-LSA) und sein Bemühen berichtet, die Bereitstellung von Geodaten datenschutzrechtlich abfedern zu lassen.

Bekanntermaßen ist die Schaffung einer GDI-LSA eingebettet in eine GDI auf der Ebene der Bundesrepublik Deutschland (GDI-DE), die Teil einer europäischen GDI sein wird. Angetrieben wird der Aufbau dieser Strukturen einerseits durch die Richtlinie 2007/2/EG des Europäischen Parlamentes und

des Rates vom 14. März 2007 (ABL.L108/1 vom 25.04.2007) zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE – Infrastructure for Spatial Information in the European Community), andererseits durch die Erkenntnis, dass in der wirtschaftlichen Nutzung staatlicher Geoinformationen ein hohes Wertschöpfungspotential liegt.

Dass die Landesregierung die Bedeutung der Bereitstellung qualifizierter Geoinformationen hoch einschätzt, zeigt sich auch darin, dass nach dem Masterplan Landesportal Sachsen-Anhalt 2007-2011 eine der Basiskomponenten der Aufbau eines Geodatenservers sein wird (vgl. IX. Tätigkeitsbericht, Nr. 4.6).

Geodaten beschreiben nicht nur die reale Umwelt und liefern Informationen zu Erscheinungen auf der Erde und unter deren Oberfläche, sie können auch, datenschutzrechtlich höchst beachtlich, den Raumbezug zu Objekten und Sachverhalten darstellen.

Beispielhaft haben solche Informationen Bedeutung für

- Katastrophenschutz
- Einsatzleitung und Notfallversorgung
- Umweltmonitoring
- Geomarketing
- Statistik
- Navigation und Verkehrsleitung
- diverse Mobil- und Auskunftsdienste.

Ohne eine GDI stehen die Anbieter von Geoinformationen, z. B. das Landesamt für Vermessung und Geoinformation, das Landesamt für Umweltschutz, der Landesbetrieb für Hochwasserschutz und Wasserwirtschaft und viele andere, auch im kommunalen Bereich, jeder für sich isoliert möglichen Nutzern dieser Geodaten, z. B. den Katastrophenschutzbehörden, gegenüber. Jeder Nutzer muss die ihn interessierenden Geodaten bei den Anbietern suchen, die Datenformate sind unter Umständen sogar proprietär.

Zwischen Anbietern und Nutzern der Geodaten wird zukünftig eine GDI eingerichtet. Anbieter und Nutzer finden sich über einen Metadatenkatalog, der Datenaustausch – nun in standardisierten Transferformaten – findet über elektronische Webdienste statt. Dabei sind natürlich datenschutzrechtliche Übermittlungs- und Veröffentlichungsvorschriften zu beachten. Bestandteile einer GDI, also auch der GDI-LSA, sind demnach neben den Geobasis- und Geofachdiensten die Metadaten zu ihrem Auffinden, die Übertragungsnetze – das wird in der Regel das Internet sein –, entsprechende Datendienste und vor allem die Rahmenbedingungen. Das sind in erster Linie Rechtsvorschriften, wie das Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt (GDIG LSA vom 14. Juli 2009, GVBl. LSA S. 368) sowie Normen und Stan-

dards, aber auch Vereinbarungen über Zugang und Nutzung, z. B. Kostenregularien, sowie Koordinierungs- und Überwachungsmechanismen.

Um in Sachsen-Anhalt eine GDI aufbauen zu können, war zunächst die Analyse der vorhandenen Geodatenbestände durch die Erfassung ihrer Metadaten durchgeführt worden. Das war mit einer netzwerkgestützten Erfassungssoftware (INGRID – Information Grid) erledigt worden. Um die Qualität und die Quantität im Sinne von Vollständigkeit der so erfassten Geodatenbestände bewerten zu können, wurde parallel dazu bei einem Landkreis, einer kreisangehörigen und einer kreisfreien Stadt und einem Gewässerunterhaltungsverband eine vertiefte Analyse der Geodatenbestände durchgeführt. Damit konnte auch ein vom Landesbeauftragten im Zusammenhang mit dem GDIG LSA gemachter Vorschlag umgesetzt werden, Art und Umfang der von Kommunen außerhalb des Anwendungsgebietes des GDIG LSA gespeicherten Geodaten festzustellen. Die Stichproben sind natürlich noch nicht aussagekräftig. Die Bewertung dieser Datenbestände durch das Ministerium des Innern unter Beteiligung des Landesbeauftragten (s. Stellungnahme der Landesregierung zum IX. Tätigkeitsbericht, Nr. 4.9) steht aus.

11.2 Datenschutz bei Öffentlich bestellten Vermessungsingenieuren

Das Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt (VermGeoG LSA) sieht in § 21 Abs. 3 vor, dass auch an den dazu Berechtigten bei den Öffentlich bestellten Vermessungsingenieuren (ÖbVI) des Landes über Online-Verfahren oder direkt über das Internet Auszüge aus dem Geobasisinformationssystem abgegeben werden können. Teil des Geobasisinformationssystems des Landes ist neben dem geotopografischen Basisinformationssystem mit den Luftbildern der Landesluftbildsammlung das aus dem Liegenschaftsbuch, der Liegenschaftskarte und der Sammlung der Vermessungszahlen bestehende Basisinformationssystem Liegenschaftskataster. Der automatisierte Abruf von Daten aus dem Basisinformationssystem Liegenschaftskataster erfolgt mit dem Geodatendienst Liegenschaftskataster, einem Service im Rahmen der E-Government-Initiative des Landes Sachsen-Anhalt. Da beim Abrufen der Liegenschaftsdaten regelmäßig auch personenbezogene Daten der betroffenen Eigentümerinnen und Eigentümer übermittelt werden, qualifiziert dies das Basisinformationssystem Liegenschaftskataster zu einem automatisierten Abrufverfahren nach § 7 DSG-LSA mit vom Gesetzgeber vorgesehenen Beschränkungen in Bezug auf die Einrichtung und den Betrieb des Abrufverfahrens.

Der Landesbeauftragte war nun der Frage nachgegangen, ob es datenschutzrechtlich geboten sein könnte, den Zugriff eines ÖbVI auf die Daten der Liegenschaften im Landkreis seines Amtssitzes zu beschränken, ob also datenschutzrechtliche Bedenken dagegen bestehen, ihm Zugriff auf den landesweiten Datenbestand zu gewähren. So sollte die grundsätzliche Frage beantwortet werden, ob Gründe dafür oder dagegen sprechen, einem ÖbVI mit Amtssitz in Salzwedel den Zugriff auf die Daten eines Flurstückes im Burgenlandkreis, ca. 250 km von seinem Amtssitz entfernt, zu gewähren.

Eine umfassende Antwort zu finden, bedarf der differenzierten Betrachtung des Sachverhaltes:

Nach § 7 Abs. 1 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) darf ein automatisiertes Abrufverfahren zur Übermittlung personenbezogener Daten nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Der Gesetzgeber hat dieser Einschränkung und der in § 7 Abs. 1 Satz 2 DSG-LSA normierten Pflicht zur Vorabkontrolle nach § 14 Abs. 2 DSG-LSA zufolge durchaus erkannt, dass von solchen Abrufverfahren ein erhöhtes Gefährdungspotential für das Persönlichkeitsrecht der Betroffenen ausgehen kann. Das gilt im Übrigen besonders vor dem Hintergrund, dass die Verantwortlichkeit für die Zulässigkeit der Übermittlung, die auf Ersuchen eines Dritten erfolgt, von der übermittelnden Stelle auf den Dritten als Empfänger der Daten übergeht (§ 7 Abs. 4 Satz 1 DSG-LSA).

Zusätzlich relevant sind die zu § 7 DSG-LSA erlassenen Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger (VV-DSG-LSA). Nach Nr. 7.1 der VV-DSG-LSA sind die wesentlichen Merkmale der Angemessenheitsprüfung vor der Einrichtung des Abrufverfahrens neben der Sensibilität der Daten, die Dringlichkeit und die Häufigkeit der begehrten Datenübermittlungen.

Auf der anderen Seite ist beachtlich, dass nach § 4 des Gesetzes über die Öffentlich bestellten Vermessungsingenieure im Land Sachsen-Anhalt (ÖbVermIngG LSA) dem ÖbVI zwar ein bestimmter Ort als Amtssitz zugewiesen worden ist, an dem er seine Geschäftsstelle einzurichten hat, sein Amtsbezirk nach § 4 Abs. 1 ÖbVermIng LSA aber das Land Sachsen-Anhalt ist. Schon insofern, und damit teilt der Landesbeauftragte die Meinung des Ministeriums des Innern, wäre es nicht angemessen, im Liegenschaftskataster den Zugriff des ÖbVI auf die Daten eines bestimmten Landkreises zu beschränken. Im Übrigen, und auch darauf wies das Ministerium des Innern hin, stelle das Vorhalten des Abrufverfahrens für die ÖbVI im landesweiten Umfang ein zwingendes Erfordernis dar, da sich das Landesamt für Vermessung und Geoinformation aus der Fläche zurückziehe, gleichzeitig aber sichergestellt werden müsse, dass den Bürgerinnen und Bürgern gegenüber weiterhin die Verwaltungsaufgaben, z. B. die Erstellung von Auszügen aus dem Liegenschaftskataster gem. § 21 Abs. 3 VermGeoG LSA, in gewohntem Umfang erbracht werden.

Datenschutzrechtlichen Vorgaben soll dabei dadurch Rechnung getragen werden, dass durch die ÖbVI Auszüge aus dem Liegenschaftskataster nur in den Fällen an Dritte abgegeben werden, in denen diese ein berechtigtes Interesse darlegen können (§ 13 Abs. 1 Satz 2 VermGeoG LSA).

Nach Würdigung aller genannten Umstände und der Tatsache, dass die 49 betroffenen ÖbVI pro Jahr mehrere tausendmal den Geodatendienst Liegenschaftskataster im Rahmen ihrer Amtsführung nutzen, hat der Landesbeauftragte keine durchgreifenden datenschutzrechtlichen Bedenken gegen das Abrufverfahren mehr.

12 Gesundheitswesen

12.1 Krankenhausinformationssysteme

Die elektronische Datenverarbeitung macht auch vor den Krankenhauseinfahrten nicht Halt. Krankenhausinformationssysteme sind inzwischen Standard. Sie bieten schnellstmöglich die benötigten Informationen zum Patienten an allen erforderlichen Orten. Der kurzfristige Zugriff aller Mitwirkenden an verschiedenen Orten wird im Interesse flexibler und interdisziplinärer Behandlung gewährleistet. Strukturen und Prozesse im Krankenhausalltag nutzen moderne Kommunikationssysteme. Die einzelnen Einheiten werden größer, der Vernetzungsgrad nimmt zu.

Dies birgt auch Gefahren für die Patientendaten, wie Erfahrungen der Datenschutzaufsichtsbehörden und bekannte Missbrauchsfälle belegen. Beobachtet wurde u. a., dass alle Ärzte eines Krankenhauses Zugriff auf alle Patientendaten hatten oder dass eine Protokollierung des Zugriffs fehlte, die eine Überprüfung hätte ermöglichen können. Auch Löschungsverfahren bzw. die Speicherdauer sind von Bedeutung (ohne Weiteres Zugriff auf die Patientenhistorie bei einer neuen Aufnahme?). Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten aber, einen Zugriff auf Patientendaten nur insoweit zuzulassen, wie dies für die konkrete Behandlung bzw. ihre verwaltungsmäßige Abwicklung erforderlich ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher im Oktober 2009 die Entschließung „Krankenhausinformationssysteme datenschutzgerecht gestalten!“ gefasst (**Anlage 3**).

Die Arbeitskreise Technische und organisatorische Datenschutzfragen sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder richteten im Herbst 2009 eine Unterarbeitsgruppe Krankenhausinformationssysteme ein. Vertreter der Kirchen waren beteiligt. Auch der Landesbeauftragte hat in der Unterarbeitsgruppe mitgewirkt. Ziel der Unterarbeitsgruppe war die Erstellung einer bundesweiten Orientierungshilfe, die einheitliche Anforderungen an ein Krankenhausinformationssystem formuliert und bei den datenschutzrechtlichen Beratungen und Prüfungen als Maßstab gelten kann. Die Ausarbeitungen basierten nicht nur auf Erfahrungen der Arbeitsgruppenmitglieder. Vielmehr wurden Experten angehört, Hersteller von Krankenhausinformationssystemen beteiligt, und Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern einbezogen. Dabei ist deutlich geworden, dass der Praxisbetrieb und bestehende technische Lösungen teilweise noch hinter den Anforderungen des Datenschutzes zurückbleiben. Experten verwiesen auf finanziellen und personellen Aufwand sowie organisatorische Schwierigkeiten.

Die zwischenzeitlich erstellte und von der Datenschutzkonferenz im März 2011 zustimmend zur Kenntnis genommene Orientierungshilfe „Krankenhausinformationssysteme datenschutzgerecht gestalten und betreiben“ umfasst in einem ersten Teil die „Normativen Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus“, nebst einem Glossar. Darin werden die rechtlichen Anforderungen erläutert. In einem zweiten Teil „Technische Anforderungen“ werden Maßnahmen zur Umsetzung der rechtlichen Vorgaben dargestellt. Die Orientierungshilfe ist auf der

Homepage des Landesbeauftragten abrufbar. Damit liegt nunmehr eine fundierte Grundlage vor, die den Prozess der Umsetzung der datenschutzrechtlichen Anforderungen stützt. Dazu hat der Landesbeauftragte auch mit der Krankenhausgesellschaft Sachsen-Anhalt Kontakt aufgenommen. Zudem beabsichtigen die Datenschutzbeauftragten des Bundes und der Länder, die weitere Entwicklung von Strukturen in Krankenhäusern zu beobachten, den Kontakt zu den Experten zu halten und ggf. Fortschreibungen der Orientierungshilfe vorzunehmen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben die Orientierungshilfe ebenfalls zustimmend zur Kenntnis genommen. Mit dem Beschluss „Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen“ vom Mai 2011 (**Anlage 29**) haben sie deutlich gemacht, das Dokument als Leitlinie bei der künftigen Bewertung konkreter Vorhaben verwenden zu wollen.

12.2 Elektronische Gesundheitskarte

Nach einer Bestandsaufnahme haben sich die Gesellschafter der Projektgesellschaft Gematik, die für die Einführung der elektronischen Gesundheitskarte (eGK) zuständig ist, im April 2010 auf einen Neustart des gesamten Systems verständigt. Die Bundesärztekammer ist hinsichtlich der Leistungserbringer (Ärzte und Zahnärzte) zuständig für die medizinischen Anwendungen, wie z. B. für den Notfalldatensatz, der auf der eGK freiwillig gespeichert werden kann. Die Kostenträger (Krankenkassen) verantworten die administrativen Daten (Versichertenstammdaten). Das ursprüngliche Vorhaben, auch Rezepte elektronisch auf der eGK zu speichern, wurde zurückgestellt.

Inzwischen liegen neue Konzepte zur elektronischen Fallakte, zum elektronischen Arztbrief, Notfalldatenmanagement und Stammdatenmanagement vor. Unklar ist jedoch, wann und wo diese Konzepte getestet werden.

Die gesetzlichen Krankenkassen müssen zum 31. Dezember 2011 10% ihrer Versicherten mit der elektronischen Gesundheitskarte ausstatten, die allerdings zunächst nur den Versichertenstatus bekundet. Die Einbeziehung des Notfalldatensatzes ist erst ab 2014 geplant; der Zeitpunkt der Einführung zusätzlicher Funktionen ist weiter offen.

12.3 Einschulungsuntersuchungen/schulärztliche Untersuchungen

In Nr. 12.6 des IX. Tätigkeitsberichtes hat der Landesbeauftragte über die Beratungen hinsichtlich der Einführung einer landeseinheitlichen Datenerhebung und -verarbeitung im Rahmen von Einschulungsuntersuchungen und schulärztlichen Untersuchungen in den Gesundheitsämtern Sachsen-Anhalts berichtet. Die Landesregierung hat in ihrer entsprechenden Stellungnahme dargestellt, die Ausführungen des Landesbeauftragten bei der Abfassung eines Erlasses zu berücksichtigen. Ein solcher Erlass ist bisher jedoch nicht ergangen.

Um die Datenerhebung und -verarbeitung bei Einschulungsuntersuchungen und schulärztlichen Untersuchungen in der Praxis kennenzulernen, hat der Landesbeauftragte im Berichtszeitraum das Gesundheitsamt eines Landkrei-

ses aufgesucht. Hinsichtlich einiger Aspekte wurden Empfehlungen zur datenschutzgerechteren Verfahrensausgestaltung gegeben.

Die Akten des Kinder- und Jugendärztlichen Dienstes werden bei Verlassen der Diensträume in verschlossenen Schränken aufbewahrt. Der private Reinigungsdienst reinigt diese Räume nach Dienstschluss. Da es sich bei den in den Akten gespeicherten Daten um besonders geschützte Gesundheitsdaten handelt, sollte die Reinigung in Anwesenheit von Beschäftigten erfolgen (§ 6 Abs. 2 DSG-LSA).

Darüber hinaus war im Gesundheitsamt geregelt, dass die Akten der Kinder bis zu deren 18. Lebensjahr dort verbleiben und dann im sog. Medizinalarchiv des Landkreises weitere zehn Jahre aufbewahrt werden. Eine Speicherung der Untersuchungsdaten der Kinder bis zum 28. Lebensjahr, obwohl mehrheitlich eine letzte Untersuchung in der 6. Klasse, d. h. mit ca. 12 Jahren, erfolgte, erschien zur Erfüllung der Verwaltungsaufgaben nicht zwingend erforderlich (§ 16 Abs. 2 Nr. 2 DSG-LSA). Das Gesundheitsamt schlug daraufhin vor, die Akten direkt nach der schulärztlichen Untersuchung in der 6. Klasse an das Medizinalarchiv zu geben. Das Medizinalarchiv würde dann entscheiden, wie lange die Akten dort verbleiben und sie nach Ablauf der Aufbewahrungsfrist vernichten. Da es sich bei dem Medizinalarchiv wohl auch um eine Verwaltungsregistratur in Verantwortung des Gesundheitsamtes handelt, wurde empfohlen, die Aufbewahrungsfristen für die jeweiligen Datenbestände konkret festzulegen und die gebotene und datenschutzkonforme Löschung zu kontrollieren. Außerdem hat der Landesbeauftragte auf das verpflichtende Angebot der Verwaltung an das zuständige archivrechtliche Archiv vor der Löschung hingewiesen (§ 11 Archivgesetz des Landes Sachsen-Anhalt).

In dem vom Gesundheitsamt genutzten Programm Octoware sind die sensiblen Gesundheitsdaten der Betroffenen ebenfalls enthalten. Hierzu wurde mitgeteilt, dass auch im Programm eine Archivierung vorgesehen ist, die durch einen Haken in einem Feld im Datensatz gekennzeichnet ist. Allerdings sei der Zugriff vom Arbeitsplatz dann wieder möglich, wenn man den Haken anklickt und dieser sodann verschwindet. Wie lange die Daten im Server gespeichert werden, war nicht bekannt.

Hierzu wies der Landesbeauftragte hin, dass die gebotene Löschung von nicht mehr erforderlichen Daten natürlich auch die elektronisch gespeicherten Daten betrifft. Der Haken für die „Archivierung“ verändert nicht die Verantwortlichkeit des Gesundheitsamtes für den gesetzeskonformen Umgang mit den Daten. Demgemäß wurde das Gesundheitsamt aufgefordert, auch für die jeweils gebotene Löschung der elektronisch gespeicherten Daten Sorge zu tragen.

12.4 Novellierung des Maßregelvollzugs

Bereits im IX. Tätigkeitsbericht (Nr. 12.3) wurde die frühzeitige Beteiligung des Landesbeauftragten bei der Erarbeitung eines Entwurfs für ein neues Maßregelvollzugsgesetz dargestellt.
Die ersten Beratungen bezogen sich auf die Berücksichtigung der ärztlichen Schweigepflicht sowie der Ausgestaltung von Fragen zur Videoüberwachung,

zur Erhebung und Speicherung von Daten von Besuchern und zur Beschränkung der Rechte der Betroffenen.

Zu Beginn des Berichtszeitraumes konnten die Beratungen des zuständigen Sozialministeriums abgeschlossen werden.
Zunächst ist angeregt worden, ergänzend zu evtl. spezifischen datenschutzrelevanten Regelungen einen Verweis auf die Regeln des DSG-LSA vorzusehen. Dies stellt einmal sicher, dass Rechtsgrundlagen für evtl. notwendige Maßnahmen zumindest auf subsidiärer Ebene klar definiert sind. Zudem wird jenseits bereichsspezifischer Regelungen ein angemessener Ausgleich zwischen den fachlichen Erfordernissen und den Interessen der Betroffenen gewährleistet. Die bisherige Regelung verwies lediglich auf das Gesetz über die öffentliche Sicherheit und Ordnung, insbesondere dessen datenschutzrechtliche Bestimmungen.

Weiter wurden konkrete Rechtsgrundlagen für spezifische, regelmäßig anstehende Aufgaben des Maßregelvollzuges erörtert. Dem ist durch detaillierte Regelungen zu Dokumentationen, Datenerhebungen und Verarbeitungen sowie Datennutzungen Rechnung getragen worden. Auch insoweit führten die Erörterungen und Beratungen zur Optimierung des Gesetzentwurfes.
So war beispielsweise für die Datenerhebung zur Identifizierung neben herkömmlichen Merkmalen wie Name und Geschlecht zunächst vorgesehen, Messungen zu gestatten. Diese pauschale Befugnis wurde aus Gründen der Erforderlichkeit und zur Datenvermeidung auf Messungen hinsichtlich Körpergröße und Gewicht beschränkt.

Die vorgesehene Befugnis zur Datenerhebung durch optisch-elektronische Einrichtungen war ebenfalls Gegenstand intensiver Erörterungen und konnten verbessert werden. So wurde zunächst darauf hingewiesen, dass der Personenkreis der zu Beobachtenden nicht näher definiert war. Da auch Mitarbeiter in den Kreis der durch Video Beobachteten einbezogen sein konnten, wurde auf die höchstrichterliche Rechtsprechung zur Beobachtung bzw. Aufzeichnung in Bezug auf Mitarbeiter Bezug genommen.
Es konnte eine Verpflichtung zur Löschung von Aufzeichnungen nach spätestens zwei Werktagen erreicht werden, wenn kein den Beobachtungszweck betreffendes Ereignis eine längere Aufbewahrung im konkreten Einzelfall erforderlich machte. Zudem wurde erläutert, dass evtl. Videoaufzeichnungen grundsätzlich einer Zweckbindung unterliegen müssen. Maßgeblich für die Verwendung können nur die sicherheitsrelevanten Aufzeichnungszwecke, nicht jedoch andere, beispielsweise personalwirtschaftliche Zwecke sein.
Ergänzend wurde darauf hingewiesen, dass die Videobeobachtung von Wohn- bzw. Schlafräumen im Hinblick auf den Kernbereich privater Lebensgestaltung bedenklich wäre. Die Beobachtung herkömmlicher Wohn- und Schlafräume sollte klar vermieden werden. Sowohl vom Gesetzeswortlaut wie von der Begründung her sollte deutlich werden, dass die aus Sicherheitsgründen (Selbstschutz) gebotene Beobachtung nur ausnahmsweise und in gesonderten Räumen durchgeführt werden kann, auch wenn diese Räume aus therapeutischen Gründen einen wohnraumähnlichen Komfort aufweisen.

Intensiv diskutiert wurde auch die Frage der Einsicht der Untergebrachten in die sie betreffenden Akten im Hinblick auf die Beeinträchtigungen des Gesundheitszustandes und Gefährdungen Dritter. Nach der Rechtsprechung

des Bundesverfassungsgerichts (Beschluss vom 9. Januar 2006, 2 BvR 443/02) steht jedem Patienten gegenüber seinem Arzt bzw. Krankenhaus grundsätzlich ein Anspruch auf Einsicht in die ihn betreffenden Krankenunterlagen zu. Dies Recht besteht zwar nicht ohne Einschränkungen, das Selbstbestimmungsrecht des Patienten muss aber nur zurücktreten, wenn ihm entsprechend gewichtige Belange entgegenstehen. Lediglich Beeinträchtigungen des Gesundheitszustandes dürften ein wohlmeinendes Vorenthalten von Informationen nicht rechtfertigen. Eventuellen Bedenken kann durch die Eröffnung der Informationen im Beisein eines Arztes begegnet werden. Lediglich Gefahren auf dem Niveau konkreter Suizidgefahren dürften daher dem Einsichtsrecht Grenzen setzen (siehe § 2 Abs. 2 der beschlossenen Gesetzesfassung).

Im Weiteren hatte der Landesbeauftragte Gelegenheit, vor dem Ausschuss für Soziales des Landtags von Sachsen-Anhalt zum Regierungsentwurf (LT-Drs. 5/2263) ausführlich auf die aus datenschutzrechtlicher Sicht bedeutsamen Aspekte hinzuweisen. Von besonderer Bedeutung war dabei die Ausgestaltung der Regelung zu Videoaufzeichnungen, die im Hinblick auf die Speicherung und vor allem die unterschiedlichen Verwendungszwecke verfassungsrechtlichen Bedenken begegnete. Im Ergebnis konnten Veränderungen erreicht werden, die unverhältnismäßigen Zweckänderungen in der Nutzung entgegenwirken (§§ 33 ff. der beschlossenen Gesetzesfassung).

Das Gesetz ist am 30. Oktober 2010 in Kraft getreten (GVBl. LSA S. 510).

12.5 Datenübermittlungen zum Schutz vor Infektionskrankheiten

Eine an offener Tuberkulose erkrankte Studentin beschwerte sich darüber, dass eine Universität zwecks Ermittlung von Kontaktpersonen Aushänge mit Namen, Geburtsdatum und Erkrankung der Petentin und der Aufforderung, sich bei Kontakt mit dem Gesundheitsamt in Verbindung zu setzen, angebracht hatte.

Nachdem sowohl das Gesundheitsamt als auch die Universität Stellung genommen haben, stellte sich der Sachverhalt für den Landesbeauftragten wie folgt dar:

Trotz des von der Petentin dem Gesundheitsamt zur Verfügung gestellten Seminarplanes konnten keine Kontaktpersonen ermittelt werden, da die Dozenten bei offenen Kursen keine Angaben zu den Teilnehmern erheben. Eine namentliche Aufstellung der Studenten durch die Petentin war ebenfalls nicht möglich. Daraufhin hat sich das Gesundheitsamt an die Universitätsleitung mit der Bitte um eine entsprechende Erfassung der Kontaktpersonen, z. B. durch Aushängen der Seminarpläne, gewandt. Die Universität hat sich allerdings trotz der Einwände des Gesundheitsamtes dazu entschlossen, die persönlichen Daten der Petentin auszuhängen.

Das Gesundheitsamt ist nach § 25 Abs. 1 Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (IfSG) u. a. verpflichtet, die Ausbreitung der Krankheit zu ermitteln. Hierdurch werden die Bestimmungen des Datenschutzes und der ärztlichen Schweigepflicht eingeschränkt, damit die Ziele des Infektionsschutzes erreicht werden können.

Dies darf jedoch nur in dem Ausmaß erfolgen, das unter Anlegung eines strengen Maßstabes für die Erfüllung des gesetzlichen Auftrages unvermeidbar ist.

Das Gesundheitsamt ist somit nach § 11 Abs. 1 DSG-LSA berechtigt, Dritte (hier die Universität) an den Ermittlungen zu beteiligen, soweit dies erforderlich ist. Die zu übermittelnden Daten sind dabei auf das unerlässliche Minimum zu beschränken.

Eine Übermittlung des Patientennamens durch das Gesundheitsamt war im vorliegenden Fall bei der erbetenen Kontaktpersonenermittlung durch die Universität wohl erforderlich. Inwieweit auch die genaue Bezeichnung der Krankheit ebenfalls unerlässlich zur Recherche war, schien zumindest zweifelhaft. Um die Wichtigkeit und Dringlichkeit der Ermittlungen sowohl der Universität als auch den potentiellen Kontaktpersonen darzustellen, hätte die Mitteilung, dass eine ansteckende und meldepflichtige Infektionskrankheit vorliegt, die Untersuchungen erfordert, ausreichend sein können.

Darüber hinaus war die Veröffentlichung des Namens und der genauen Krankheitsbezeichnung durch Aushänge auf dem Universitätsgelände durch die Universität datenschutzrechtlich zu betrachten. Hierbei handelte es sich um Datenübermittlungen an nicht-öffentliche Stellen. Die Zulässigkeit dieser Datenübermittlungen war ausschließlich unter den Voraussetzungen des § 12 Abs. 1 DSG-LSA gegeben. Diese schienen jedoch weder für die Datenübermittlung des Namens noch der Krankheit vorzuliegen. Eine Datenübermittlung muss sich immer am Grundsatz der Erforderlichkeit messen lassen, d. h. die zu übermittelnden Daten müssen nicht nur hilfreich, sondern vielmehr unerlässlich zu Aufgabenerfüllung sein. Im vorliegenden Fall hätte ein anonymer Aushang des Seminarplans ausgereicht, um die Studenten um Meldung im Dekanat zu bitten, die ebenfalls in diesen Vorlesungen waren. Im Dekanat hätte dann die Information zur Meldung beim Gesundheitsamt erfolgen können. Gegebenenfalls hätte auch bereits der Aushang über eine ansteckende und meldepflichtige Infektionskrankheit Auskunft geben können, um die Bedeutung der Meldepflicht hervorzuheben. Ein personenbezogener Aushang, ob mit oder ohne Krankheit, wäre nicht erforderlich gewesen.

Zusammenfassend war damit festzustellen, dass insbesondere die Universität mangels hinreichender Vorgaben und aus Sorge um die Gesundheit der Studierenden überreagiert hat. Der Landesbeauftragte hat deshalb das Gesundheitsamt aufgefordert, die Prüfung der Erforderlichkeit, welche Patientendaten im Einzelfall zur Kontaktpersonenermittlung tatsächlich an Dritte zu übermitteln sind, zukünftig strikter durchzuführen und die umsetzenden Stellen, die nicht über die diesbezüglichen Erfahrungen des Gesundheitsamtes verfügen, entsprechend zu beraten. Auch die Universität wurde darum gebeten, die datenschutzrechtlichen Vorschriften zukünftig genauer zu beachten und die Beschäftigten entsprechend zu sensibilisieren.

12.6 Gendiagnostikgesetz

Am 1. Februar 2010 trat das Gendiagnostikgesetz in Kraft (BGBl. I 2009 S. 2529), das gendiagnostische Untersuchungen reguliert und die Abfrage von entsprechenden Untersuchungsergebnissen u. a. durch Arbeitgeber und

Versicherungen sehr stark einschränkt (Überblick zum Gesetzesinhalt bei Genenger, NJW 2010, 113). In § 22 des Gendiagnostikgesetzes werden die Regelungen für Beschäftigte für verbeamtete Bedienstete für entsprechend anwendbar erklärt. Dies bezieht sich jedoch wohl lediglich auf Bundesbedienstete. So sieht auch die Begründung des Entwurfs der Bundesregierung zu § 22 (BT-Drs. 16/10532, S. 39) vor, dass die Regelungen für Dienstverhältnisse „des Bundes“ entsprechend gelten. Demnach wären nicht verbeamtete Beschäftigte im öffentlichen Dienst der Länder als Arbeitnehmerinnen und Arbeitnehmer nach § 3 Nr. 12 a) Gendiagnostikgesetz von den Regelungen erfasst, nicht jedoch die Landesbeamten.
Dem Wortlaut nach könnte daher eine Regelungslücke angenommen werden, worauf der Landesbeauftragte das Ministerium des Innern hinwies. In Nr. 28.1.1 VV-DSG-LSA wurde daraufhin eine Ergänzung vorgenommen, die klarstellt, dass auch die verbeamteten Bediensteten entsprechend dem engen Rahmen des Gendiagnostikgesetzes geschützt sind.

Das Gendiagnostikgesetz umfasst nicht den Bereich der Forschung etwa im Bereich der Biobanken (vgl. VIII. Tätigkeitsbericht, Nrn. 9.4, 9.5). Der Deutsche Ethikrat hat im Juni 2010 u. a. die Einführung eines Biobankgeheimnisses empfohlen (BT-Drs. 17/2620). Forderungen nach einer gesetzlichen Regelung für die genetische Forschung haben sich verstärkt, so u. a. durch das Büro für Technikfolgenabschätzung (BT-Drs. 16/5374) und Anträge der Opposition im Bundestag (BT-Drs. 17/3790 und 17/3868 – mit weiteren Nachweisen).

12.7 Landeskrebsregister

Neue Tumorerkrankungen sind auf staatsvertraglicher Grundlage in dem dort genannten Umfang an das Gemeinsame Krebsregister der fünf neuen Bundesländer und Berlin zu melden. Dieses epidemiologische, also bevölkerungsbezogene Register kann Aussagen über das Auftreten und die Häufigkeit von Krebserkrankungen treffen. Der Gesetzgeber hat dem Patienten insoweit aber ein Widerspruchsrecht eingeräumt, worüber er zu informieren ist.

Daneben existieren in Sachsen-Anhalt drei klinische Krebsregister (Tumorzentren) in Magdeburg, Halle und Dessau-Roßlau. Dort werden krankheitsbezogene Daten der Patienten in größerem Umfang als im Gemeinsamen Krebsregister gespeichert. Durch Langzeitbeobachtung werden Aussagen über die Qualität der Früherkennung, der Diagnostik und der Therapie und damit auch Auswertungen z. B. für die Versorgungsforschung möglich. In den klinischen Registern werden die Patientendaten namensbezogen auf der Grundlage der Einwilligung der Betroffenen gespeichert.

Nunmehr ist geplant, die umfänglichen medizinischen Daten in einem landesweiten Register zusammenzuführen. Es soll ein Überblick über die individuellen Krankheitsverläufe aller Erkrankten ermöglicht werden, auch wenn die Behandlung oder Therapie im Einzugsbereich mehrerer regionaler Register erfolgte. So kann auch die Behandlungsqualität im ganzen Land abgebildet werden. Ein Rückschluss auf die einzelne Person soll dabei aber ausgeschlossen werden. An dem Vorhaben wurde der Landesbeauftragte durch die Otto-von-Guericke Universität Magdeburg frühzeitig beteiligt.

In den Beratungen wurde zunächst festgestellt, dass, soweit personenbeziehbare Daten Verwendung finden, mangels gesetzlicher Grundlage eine Einwilligung erforderlich ist. Um als Rechtsgrundlage tragfähig zu sein, muss die Einwilligung neben der Freiwilligkeit auf einer hinreichenden Aufklärung über die beabsichtigte Datenverwendung basieren. Auf die gebotene Transparenz wurde hingewiesen. Dabei war aber auch zu berücksichtigen, dass den Patienten angesichts einer besonders bedrückenden Diagnose keine langen und differenzierten Datenfluss- und Datensicherheitskonzepte zuzumuten sind. Die Ausgestaltung einer Einwilligungserklärung und eines zusätzlichen Informationsflyers wurde eingehend erörtert.

Weiterhin sollten aber auch die Daten der Patienten in das neu zu schaffende Landeskrebsregister einbezogen werden, die in den regionalen Register bereits erfasst sind, deren bisherige Einwilligung die landesweite Zusammenführung von Daten aber nicht umfasst. Hierzu hat die Universität ein Konzept entwickelt, dass mittels eines sog. Hashverfahrens zu einem Pseudonym (Kontrollnummer) führt, zu dem mittels dieses Verfahrens weitere medizinische Daten hinzugefügt werden können. Ein Rückschluss aus der Kontrollnummer auf die Ausgangsdaten ist nicht möglich. Mit Hilfe eines sog. Recordlinkagetools werden dann Dubletten erkannt und die medizinischen Daten korrekt der der betroffenen Person entsprechenden Kontrollnummer zugeordnet. Die Daten werden dann ohne die Kontrollnummer auf Rechner transferiert, die von außen zugänglich sind. Ein umfänglicher medizinischer Datensatz steht den Leitern der drei an dem Landeskrebsregister beteiligten klinischen Krebsregister zur Verfügung. Ein sehr kleiner Datensatz steht allgemein über einen Internetserver zur Verfügung.

Hierzu hat der Landesbeauftragte die Universität in technisch-organisatorischer Hinsicht umfänglich beraten. Dabei ging es u. a. darum, zu verhindern, dass durch den Datenumfang oder die Erkennbarkeit von Kontrollnummern den Leitern der drei Einrichtungen die Herstellung des Personenbezuges zu Einzelfällen ermöglicht wird, die nicht nur in der eigenen Region behandelt wurden. Die Beratungen dauern noch an.

12.8 Neugeborenenscreening

Zur Früherkennung von angeborenen Stoffwechseldefekten und endokrinen Störungen bei Neugeborenen sieht die Kinderrichtlinie des Gemeinsamen Bundesausschusses (s. §§ 90, 91 SGB V) in der Gesetzlichen Krankenversicherung ein Neugeborenenscreening vor. Dazu werden in der Regel im Laufe des zweiten oder dritten Lebenstages aus der Ferse einige Blutstropfen entnommen und auf eine Karte geträufelt, die in ein zentrales Screeninglabor zur Untersuchung gesandt wird. Die Zielerkrankungen sind seltene, angeborene Erkrankungen, die nicht durch äußere Zeichen erkennbar sind, bei kurzfristiger Behandlung jedoch in ihren Auswirkungen erheblich gemildert werden können. Das Screeningzentrum in Sachsen-Anhalt ist in der Universitätskinderklinik in Magdeburg angesiedelt. Da nach der Kinderrichtlinie eine bestimmte Größe des Zentrums erforderlich ist, kooperiert das Screeninglabor mit anderen Einrichtungen in anderen Ländern (Kompetenznetz Neugeborenenscreening). Ein Zugriff auf die Daten der jeweils anderen Labore ist aber nicht möglich.

Zur Information der Eltern wurden ein zweiseitiges, umfängliches Informationsblatt und eine zweiseitige, mit Erläuterungen versehene Einverständniserklärung als Rechtsgrundlage für das Neugeborenenscreening verwandt.

Bei einem Besuch des Screeningzentrums hat der Landesbeauftragte festgestellt, dass zum Teil noch Restblutproben aus den 90er Jahren in den Kellerräumen lagerten. Ältere Blutproben waren noch direkt mit den personenbezogenen Daten versehen. Seit ca. 2003/2004 wurden Filterpapierkarten verwandt, bei denen die Restblutproben von den personenbezogenen Daten abgetrennt werden konnten. Die Restblutproben sind daher lediglich mit einer Nummer versehen. Seit 2006 wird eine Screening-ID verwendet. Die Screening-ID wird vom Einsender auf der Filterpapierkarte vermerkt. Die Software einer Firma aus Dresden generiert diese ID für Einsender mehrerer Bundesländer.
Spätestens am Tag nach der Laboruntersuchung werden die beiden Teile voneinander getrennt und die Blutproben im abgeschlossenen Keller in einem verschlossenen Schrank aufbewahrt. Wird in der Einverständniserklärung angekreuzt, dass die Aufbewahrung der Blutprobe abgelehnt wird, wird sie sofort vernichtet. Eine längere Aufbewahrung scheint aber aus unterschiedlichen Gründen wünschenswert (Hilfe bei Spätmanifestationen, Klärung von Haftungsfragen).
Die personenbezogenen Daten verbleiben bis zur Abrechnung im Labor. Wenn die Abrechnung erfolgt ist, werden diese Teile der Filterpapierkarte auch im Keller in einem anderen Schrank verschlossen aufbewahrt. Einen Schlüssel hat nur die Laborleiterin.
Die Vergabe einer Screening-ID ist nach Auffassung des Screeningzentrums erforderlich, um den Erstbefund eines Kindes auch dem Zweitbefund zuordnen zu können. Es ist z. B. möglich, dass Kinder bei Zusendung des Zweitbefundes einen neuen Nachnamen haben oder zwei Kinder in derselben Klinik am selben Tag denselben Namen erhalten.

Der Landesbeauftragte hat das Screeningzentrum umfänglich u. a. wie folgt beraten:

Geschützte personenbezogene Informationen sind grundsätzlich sämtliche persönliche und sachliche personenbeziehbare Verhältnisse des Betroffenen. Auch wenn die Personenbeziehbarkeit von isolierten Blutproben diskussionswürdig ist (die zunehmende medizinische Verbundforschung könnte zu identifizierenden Referenzdateien führen), ist zumindest durch die Kombination mit Informationen zur Person eine Personenbeziehbarkeit auch der in den Blutproben manifestierten medizinischen Informationen gegeben. Demgemäß handelt es sich insoweit auch um Gesundheitsdaten, die einem besonderen landes-, bundes- und europarechtlichen Schutz unterliegen. Für die Verarbeitung personenbezogener Daten bedürfen öffentliche Stellen des Landes einer Rechtsgrundlage (§ 4 Abs. 1 DSG-LSA).

Eine gesetzliche spezielle Regelung als Grundlage der Durchführung des Neugeborenenscreenings durch das Universitätsklinikum in Form einer landesweiten zentralen ärztlich geleiteten Labordienstleistung erschien nicht ersichtlich. Auch die Kinderrichtlinien des Bundesausschusses der Ärzte und Krankenkassen (Bundesanzeiger 2009; Nr. 132: S. 3125) stellten keine Rechtsgrundlage dar.

Maßgeblich war daher die Einwilligung der Betroffenen, die an den Vorgaben des § 4 Abs. 2 DSG-LSA zu messen ist.

In Bezug auf die mit Namen aufbewahrten Altproben war die Grundlage der Einwilligungserklärung zu prüfen. Es erschien fraglich, ob in den alten Einwilligungserklärungen mit hinreichender Bestimmtheit auf der Grundlage entsprechender Aufklärung die langfristige personenbeziehbare Aufbewahrung von Blutproben eingeschlossen war. Beim Fehlen einer Rechtsgrundlage war die Löschung geboten (§ 16 Abs. 2 DSG-LSA).
Bezüglich der Altproben seit Verwendung der Filterpapierkarten (ca. 2003 bis 2006) war ebenfalls zu prüfen, ob eine hinreichende Rechtsgrundlage für die Speicherung einerseits der personenbezogenen Daten und andererseits der Blutprobe noch besteht. Auch hier bestanden Zweifel hinsichtlich der Bestimmtheit und Tragweite der Einwilligungen.

Die Kinderrichtlinie des Gemeinsamen Bundesausschusses enthält auch datenschutzrechtliche Aspekte. So sieht beispielsweise § 5 Abs. 2 vor, dass Daten zu solchen Krankheiten, die nicht Zielkrankheiten im Sinne des § 5 Abs. 1 sind, unverzüglich zu vernichten sind. Zudem ist ausdrücklich die Zweckbindung festgelegt. § 15 Abs. 3 sieht vor, dass Restblutproben unverzüglich nach Abschluss der Ringversuche zur Qualitätssicherung, spätestens jedoch nach drei Monaten zu vernichten sind. Für die gesetzlich versicherten Patienten waren dies nicht gesetzlich zwingende aber datenschutzrelevante Vorgaben, mit denen das bisherige Vorgehen nicht hinreichend übereinstimmte.

Die dauerhafte Aufbewahrung der Restblutproben war unzulässig. Soweit die kurzfristige Aufbewahrung der Proben aus medizinischen Gründen zwingend geboten ist, wie beispielsweise bei kurzfristigen Zweituntersuchungen von Frühgeborenen, bestehen keine datenschutzrechtlichen Bedenken. Ein Teil der mittelfristig aufbewahrten Blutproben war aber bereits durch Lagerschäden verloren gegangen, sodass schon die praktische Erforderlichkeit fraglich schien. Zudem würde die Gefahr einer landesweiten „Gendatei“ begründet. Die Einwilligung als Rechtsgrundlage fehlte bzw. schien nicht ausreichend. Dabei war zu berücksichtigen, dass die Erklärenden davon ausgehen konnten, dass herkömmlicherweise die personenbezogenen Informationen sowie Diagnose- und Befunddaten aufbewahrt werden, während Blut- und Gewebeproben in der Regel der Vernichtung anheimfallen. Zudem war zu monieren, dass von einer hinreichenden Aufklärung nicht mehr ausgegangen werden konnte, wenn der Vorgang der rein räumlichen Trennung innerhalb derselben verantwortlichen Stelle (Universitätsklinikum Magdeburg; vgl. § 2 Abs. 8 DSG-LSA) als Pseudonymisierung (vgl. § 2 Abs. 7a DSG-LSA zu den hier nicht erfüllten Voraussetzungen) bezeichnet wird. Das Universitätsklinikum als öffentliche Stelle ist im besonderen Maße der Beachtung des Verhältnismäßigkeitsgrundsatzes und der Achtung der Persönlichkeitsrechte unterworfen.

Perspektivisch wurde dargestellt, wie dem Grundrecht auf informationelle Selbstbestimmung durch die Ausgestaltung des Verfahrens Rechnung getragen werden könne. Der personenbezogene Zugriff auf die Blutproben sollte, soweit überhaupt noch möglich, ausschließlich durch die Personensorgeberechtigten veranlasst werden. Die Trennung der Unterlagen allein wäre nicht

ausreichend. Vielmehr wäre zumindest eine den gesetzlichen Anforderungen des § 2 Abs. 7a DSG-LSA genügende Pseudonymisierung vorzunehmen. Um die Herstellung des Personenbezuges der Blutprobe durch das Universitätsklinikum zu vermeiden, dürfte die Einschaltung eines ausschließlich den Weisungen der Personensorgeberechtigten unterliegenden Treuhänders geboten sein, wie es bereits in der Einverständniserklärung angedeutet war. Im Hinblick auf den Informationsgehalt, der Blutproben zukommt, sind besondere Anforderungen an die Seriosität des Treuhänders zu stellen, sodass an eine Stelle zu denken ist, die der strafrechtlich sanktionierten Schweigepflicht (öffentliche Stelle, Rechtsanwalt) unterliegt. Zudem sollten vorher Kriterien festgelegt und dem Treuhänder vorgegeben werden, die eine Reidentifizierung der Restblutproben gestatten (wie beispielsweise bei Verlangen der Eltern oder einer konkreten Gefahr für Leib oder Leben). Das Verfahren sollte präzise beschrieben werden, damit die Einwilligung der Eltern dies erfassen und sie ihre Rechte wahrnehmen können.

Ergänzend wurde auf die besondere datenschutzrechtliche Problematik von Einwilligungserklärungen hingewiesen, die die künftige Verwendung von Blut- oder Gewebeproben für allgemeine Forschungszwecke umfassen. Eine diesbezügliche Einwilligung sollte ebenfalls mit in die Erklärung aufgenommen werden.
Die Verwendung von Blutproben zu wissenschaftlichen Zwecken betraf jedoch einen völlig anderen Fragenkomplex, der das Screening nicht beeinflusst. Diese Einwilligung sollte daher optisch getrennt von der Einwilligung zum Screening erfolgen. Eine hinreichende Differenzierung sollte für die Leser möglich sein. Zudem sind an eine solche informierte Einwilligung höhere Informationsansprüche zu stellen (verantwortlicher Träger des Forschungsvorhabens, Zweck des Forschungsvorhabens, Art und Weise der Verarbeitung, Kooperationspartner, Zeitpunkt der Löschung usw.). Es sollte nicht allgemein auf Unkenntlichmachung verwiesen werden. Vielmehr sollte erläutert werden, ob und wie eine Anonymisierung oder nur Pseudonymisierung vorgesehen ist. Weitere Anforderungen könnten sich ergeben, wenn die Verwendung für im Zeitpunkt der Einwilligung noch nicht absehbare Forschungsprojekte angedacht sein sollte. Insgesamt war daher die bisherige Vermengung der Einwilligungen bedenklich.

Zur Verwendung einer Screening-ID wurde die Gefahr umfänglicher Datenverknüpfungen erörtert. Ihr ist durch eine datenschutzkonforme restriktive Ausgestaltung des Verfahrens Rechnung zu tragen. Demgemäß sollte nach Darstellung der Vordrucke eine unrechtmäßige Nutzung durch mathematische Zusammenhänge ausgeschlossen sein. Soweit sich die Verwendung auf interne Vorgänge der Universitätskinderklink beschränkt und als außenstehende Dritte lediglich die Eltern als Inhaber des Untersuchungshefts Zugang zu Daten der Kinder bekommen können, wäre die Verwendung einer solchen ID aus datenschutzrechtlicher Sicht vertretbar.
Weiter wurden Empfehlungen zur Ausgestaltung der Informations- und Aufklärungsunterlagen für die Eltern sowie die Einverständniserklärungen gegeben.

Abschließend war auch darauf hinzuweisen, dass die datenschutzrechtlich verantwortliche Stelle für die Vorgänge der Datenerhebung und Speicherung sowohl der personenbezogenen Daten als auch der Proben konkret zu be-

nennen ist (Universitätskinderklinik statt Kompetenznetz – Neugeborenenscreening). Damit können die Betroffenen ihre Rechte geltend machen.

12.9 Praxis-EDV und medizinische Netze

Medizinische Einrichtungen und medizinische Netze kommunizieren elektronisch. Ein Beispiel ist die Abrechnung in der Gesetzlichen Krankenversicherung (§ 295 Abs. 4 SGB V). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit technisch-organisatorischen Fragen bei der Anbindung an medizinische Netze befasst. Mit der Entschließung „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ vom März 2011 (**Anlage 23**) werden datenschutzrechtliche Anforderungen formuliert.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben die „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ im Mai 2011 in Beschlussform (**Anlage 30**) gefasst.

13 Gewerbe und Wirtschaft

13.1 Smart Meter/Smart Grid – Intelligente Messgeräte und mehr

Mit einem innovativen Technologiekonzept, dem sogenannten „Smart Metering“, d. h. der Möglichkeit, zukünftig durch intelligente, da vernetzte Messgeräte für Elektrizität, Gas, Wasser und Wärme den Verbrauch in bestimmten Zeitintervallen digital zu erfassen und zu verarbeiten, wird das Ziel verfolgt, auf der Basis des aktuell gemessenen Lastverhaltens der privaten Haushalte, grundsätzlich die Erzeugung von Energie zu regeln und zu optimieren. Eine solche technologische Lösung erlaubt es den Energieversorgungsunternehmen zudem, kostengünstiger, da am wirklichen Bedarf orientiert, zu produzieren. Darüber hinaus soll damit dem Verbraucher die benötigte Energie, auch unter Beachtung von Umweltgesichtspunkten durch die dann optimale Einspeisung von erneuerbaren Energien, effizient bereitgestellt werden.

So erfordern z. B. intelligente Stromnetze (Smart Grids) die Vernetzung des Verbrauchers (also des einzelnen Haushalts) mit dem jeweiligen Stromversorgungsunternehmen und bedingen dabei natürlich den Datenaustausch zwischen dem intelligenten Messgerät (Smart Meter) und dem Steuerungssystem des Versorgungsunternehmens.

Grundsätzlich stellt sich hierbei die Frage, ob diese auf den ersten Blick verbraucherfreundliche Lösung einer automatischen Verbrauchserfassung nicht durch die Möglichkeit der Erstellung präziser Verbrauchsprofile der Betroffenen auch Datenschutzbelange berührt.

Dass in diesem Regelkreislauf zwischen der Erfassung des Energieverbrauchs und der Steuerung der Energieproduktion auch personenbezogene Daten der privaten Verbraucher übermittelt bzw. verarbeitet werden, ist dabei unvermeidlich. Deshalb ist gerade hierbei ein hohes Datenschutz- und Datensicherheitsniveau von besonderer Bedeutung. Die detaillierte Erfassung des Verbrauchs in sogenannten Lastprofilen, bezüglich der Lebensgewohn-

heiten der Betroffenen in ihrem häuslichen Umfeld und die mögliche Bildung detaillierter Nutzungsprofile der Verbraucher, bergen ein hohes Ausforschungspotential in sich. Für Smart Meter/Smart Grid sind damit Prinzipien wie Vertraulichkeit, Integrität, Zweckbindung, Datenvermeidung, Datensparsamkeit, Pseudonymisierung, Anonymisierung und Transparenz zu beachten. Das Prinzip „Privacy by Design“, d. h. der Einbeziehung des Datenschutzes von vornherein in die Gesamtkonzeption solcher Vorhaben, gilt es hierbei umzusetzen.

Der Bundesgesetzgeber hat im Zuge der Öffnung des Messwesens bei Strom und Gas bereits mit einer Novelle des Energiewirtschaftsgesetzes (EnWG) vom 29. August 2008 (BGBl. I S. 1790) hierfür die gesetzlichen Voraussetzungen geschaffen, allerdings ohne im EnWG spezifische Regelungen für Datenschutz und Datensicherheit festzulegen.

Seit dem 1. Januar 2010 sind gem. § 21b Abs. 3a EnWG Messstellenbetreiber verpflichtet, „soweit dies technisch machbar und wirtschaftlich zumutbar ist“, in Gebäuden, die neu an das Energieversorgungsnetz angeschlossen werden oder bei größeren Renovierungen, Messeinrichtungen einzubauen, die den Endverbraucher über den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit informieren.

Im Gegenzug sind die Energieversorgungsunternehmen gem. § 40 Abs. 3 EnWG verpflichtet worden, „soweit dies technisch machbar und wirtschaftlich zumutbar ist“, bis spätestens 30. Dezember 2010 den Endverbrauchern von Elektrizität einen Tarif anzubieten, der „einen Anreiz zur Energieeinsparung oder zur Steuerung des Energieverbrauchs setzt“.

In der Einführungsphase soll der Verbraucher durch die Kopplung der Verbrauchsanzeige mit dem aktuellen Strompreis noch selbst handeln, indem er kostenbewusst energieintensive Geräte erst bei niedrigeren Strompreisen betreibt und damit gleichzeitig Lastspitzen vermeiden hilft. Bei der zukünftigen Umsetzung von Smart Grids soll diese Steuerung der Geräte nicht mehr interaktiv durch den Endverbraucher, sondern automatisch nach voreingestellten Präferenzen des Endverbrauchers erfolgen. Vor dem Hintergrund dieser technologischen Entwicklung hat die 80. Konferenz der Datenschutzbeauftragten des Bundes und Länder am 3. und 4. November 2010 in einer Entschließung eine stärkere Beachtung des Datenschutzes beim Einsatz von Smart Metering Systemen und dem Aufbau von Smart Grids gefordert (**Anlage 18**).

Das zuständige Bundesministerium für Wirtschaft und Technologie hat nunmehr diese datenschutzrechtlichen Defizite erkannt. Als ein erster Schritt bei der Weiterentwicklung des Rechtsrahmens für den Einsatz solcher intelligenten Stromnetze in Deutschland wurde das BSI im September 2010 vom Bundesministerium für Wirtschaft und Technologie beauftragt, detaillierte Anforderungen an die Sicherheitsarchitektur von Smart Metering Systemen, insbesondere für die Kommunikationseinheit, in einem Schutzprofil (Protection Profile) zu entwickeln, denn aus der Verarbeitung von personenbezogenen Verbraucherdaten in Smart Metering Systemen wie auch mögliche Angriffe auf Smart Grids ergeben sich hohe Anforderungen an den Datenschutz und die Informationssicherheit. Mittlerweile hat das Bundesamt für die Sicherheit

in der Informationstechnik im März 2011 den überarbeiteten 2. Entwurf dieses Schutzprofils für Smart Metering Systeme vorgestellt. Ende Mai 2011 sollte der Entwurfsprozess beendet sein. Das BSI plant, das Schutzprofil für Smart Metering Systeme im laufenden Jahr 2011 fertigzustellen.

In seiner Stellungnahme zum Änderungsentwurf des EnWG (BR-Drs. 343/11 (Beschluss) vom 17. Juni 2011) bat der Bundesrat, im weiteren Gesetzgebungsverfahren zu prüfen, ob die datenschutzrechtlichen Regelungen in § 21g des Gesetzentwurfes genügen, um das Persönlichkeitsrecht der Betroffenen, insbesondere gegen Ausforschung des Nutzerverhaltens, hinreichend zu schützen. Als weitere zusätzliche gesetzliche Festlegungen wurden Maßnahmen zur Erkennbarkeit von Fernmessdiensten für den Kunden, ein Kopplungsverbot zwischen günstigen Tarifen und Offenlegung des Nutzerverhaltens sowie die Anwendung der Bußgeldvorschriften des Bundesdatenschutzgesetzes für alle Verstöße gegen Datenschutzvorgaben des EnWG gefordert. Inwieweit die nunmehr beschlossenen gesetzlichen Vorgaben (BR-Drs. 395/11 vom 1. Juli 2011 und Gesetz vom 26. Juli 2011, BGBl. I S. 1554) im Hinblick auf den Datenschutz und die Datensicherheit ausreichen, wird die zukünftige praktische Umsetzung zeigen. Es bleibt abzuwarten, wie hierfür die Verordnungsermächtigung des § 21i EnWG genutzt wird, um die Datenschutzvorgaben des Gesetzes klar umzusetzen.

Die Europäische Kommission hat in ihrer Mitteilung vom 12. April 2011 „Intelligente Stromnetze – von der Innovation zur Realisierung“ (KOM(2011) 202 endg.; BR-Drs. 201/11 vom 12. April 2011) in der Einschätzung zur Entwicklung gemeinsamer europäischer Normen für intelligente Netze die Gewährleistung des Datenschutzes für Verbraucher als eine wesentliche Aufgabe bei der Entwicklung und Realisierung dieser intelligenten Netze bekräftigt. Den „besonderen Datenschutzmerkmalen intelligenter Netze“ soll dabei Rechnung getragen werden und die europäischen Normungsgremien sollen hierbei die technischen Normen unter Anwendung des Entwicklungsansatzes „Privacy by Design“ entwickeln.

Die Thematik der intelligenten Stromnetze gehört vornehmlich zum Zuständigkeitsbereich der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich.

Intelligente Stromnetze stehen dabei beispielhaft erst für den Anfang einer technologischen Entwicklung, denn weitergehende Innovationskonzepte werden bereits vom Bundesministerium für Wirtschaft und Technologie im Zusammenwirken mit nationalen Normungsgremien und den Unternehmen erörtert. Unter dem Motto „Einfach, intelligent, vernetzt – starke Marken setzen Zeichen für die Zukunft des **Smart Home**“ werden bereits Möglichkeiten für das intelligent vernetzte Haus diskutiert. Auch hierfür müssen Belange des Datenschutzes und der Datensicherheit von Beginn an Berücksichtigung finden. Der Landesbeauftragte wird jedenfalls die technologischen Entwicklungen in diesen Themenbereichen weiterhin aufmerksam verfolgen.

Bereits in seinem VIII. Tätigkeitsbericht (Nr. 4.4) hatte sich der Landesbeauftragte mit einer anderen „smarten“ Technologie, der **RFID-Technologie**, befasst. Hier hat es eine positive Weiterentwicklung gegeben. Die Europäische Kommission hat in einer Empfehlung vom 12. Mai 2009 zur Umsetzung der

Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen entsprechende Hinweise an die Mitgliedsländer herausgegeben (ABl. EU L122 S. 47). Nach Ablauf von zwei Jahren sollen danach die Mitgliedstaaten der Kommission Mitteilung über die von ihnen eingeleiteten Maßnahmen zur Umsetzung der Empfehlungen machen. Mit einer Entschließung hatte bereits der Bundesrat am 18. März 2011 (BR-Drs. 48/11 (Beschluss)) darauf gedrängt, den RFID-Einsatz verbrauchergerecht und unter Beachtung des Datenschutzes zu gestalten. Weiterhin wurde in diesem Beschluss die Bundesregierung aufgefordert, wieder Verhandlungen mit der Wirtschaft über eine Selbstverpflichtung beim RFID-Einsatz aufzunehmen. Diese Selbstverpflichtung soll u. a. Vorgaben für die Kennzeichnung, Verbraucherinformation, für Datenschutzkonzepte und Deaktivierungsmöglichkeiten der RFID-Chips enthalten.

Die Europäische Kommission hat am 6. April 2011 eine Selbstverpflichtung der Wirtschaft zur Sicherung der Privatsphäre beim RFID-Einsatz (Datenschutz-Folgenabschätzung; Privacy Impact Assessment – PIA) gebilligt und damit diesem Selbstregulierungskodex der Wirtschaft zugestimmt, der die Empfehlungen der Europäischen Kommission vom 12. Mai 2009 umsetzt. Die weitere Praxis des RFID-Einsatzes wird zeigen, ob dieser Selbstregulierungsmechanismus ausreichend ist, der vor dem RFID-Einsatz die Abschätzung der Risiken für das informationelle Selbstbestimmungsrecht der Verbraucher verlangt.

13.2 Bekämpfung von Schwarzarbeit und illegaler Beschäftigung

Unter dem Namen OWiSch – Datenbank für Erfassung von Ordnungswidrigkeiten im Bereich der Schwarzarbeitsbekämpfung der niedersächsischen Kommunen wird, so teilte das Ministerium für Wirtschaft und Arbeit dem Landesbeauftragten mit, in Niedersachsen ein automatisiertes Verfahren betrieben, in dem anhängige oder beendete Bußgeldverfahren im Hinblick auf Schwarzarbeit und unzulässige Handwerksausübung gespeichert werden. Für Sachsen-Anhalt solle ein vergleichbares Verfahren aufgebaut werden. Eine solche Ankündigung, untersetzt mit aussagefähigen Unterlagen und nicht, wie im vorliegenden Fall ausschließlich mit einer niedersächsischen PowerPoint-Präsentation, würde der Landesbeauftragte als Unterrichtung nach § 14 Abs. 1 Satz 2 DSG-LSA ausdrücklich begrüßen. Sie böte ihm die Möglichkeit, auf datenschutzrechtlich relevante Designfehler des beabsichtigten Verfahrens aufmerksam machen zu können, bevor deren spätere Beseitigung ins Kontor schlägt. Da die Schwarzarbeit nicht an der Landesgrenze aufhöre, wäre es sinnvoll, die Datenbank mit Niedersachsen gemeinsam zu betreiben, sei doch jene Datenbank mit Hilfe des dortigen Landesbeauftragten für den Datenschutz aufgebaut worden. Das war zwar, so ergab eine Nachfrage, nicht ganz richtig, gleichwohl wurde dem Landesbeauftragten von seinem niedersächsischen Kollegen dankenswerterweise eine Fülle von – allerdings niedersächsischen – Unterlagen zur Verfügung gestellt.

Aufgrund dieser Informationslage gab der Landesbeauftragte gegenüber dem Ministerium für Wirtschaft und Arbeit eine erste Stellungnahme ab, dass das Projekt keinen durchgreifenden datenschutzrechtlichen Bedenken begegne, obgleich es verbesserungswürdig sei. Tatsächlich ist es so, dass ein solches Verfahren mit Landesgrenzen übergreifender Datenbankanbindung

nach dem Schwarzarbeitsbekämpfungsgesetz (SchwarzArbG) und der Handwerksordnung (HWO) für die nach Landesrecht zuständigen Behörden gem. § 12 Abs. 1 Nr. 2 SchwarzArbG auf der Grundlage von § 49c OWiG i. V. m. § 486 StPO betrieben werden könnte. Änderungsbedarf sah der Landesbeauftragte u. a. in der Absicht, im OWiSch auch anhängige Bußgeldverfahren, also bisher unbewiesene Verdachtsfälle, zu speichern. Darin liegt eine mögliche Benachteiligung der Betroffenen bei der Vergabe öffentlicher Aufträge. Das gilt auch für die zwei Jahre fortwährende Speicherung von rechtskräftig Freigesprochenen. Für diese Fälle lässt OWiSch jede Erforderlichkeit missen.

Dann schien sich 17 Monate lang in der Sache nichts mehr getan zu haben, bis wieder Post vom niedersächsischen Datenschutzbeauftragten kam. Der sandte dem Landesbeauftragten den Entwurf einer „Verwaltungsvereinbarung zwischen dem Land Niedersachsen und dem Land Sachsen-Anhalt über die gemeinsame Nutzung einer Webanwendung mit zentraler Datenbankanbindung zur Erfassung von Ordnungswidrigkeiten“, in der es um OWiSch ging. Doch waren die Hinweise und Warnungen des Landesbeauftragten gegenüber dem Ministerium für Wirtschaft und Arbeit in keiner Weise beachtet worden. Im Gegenteil: Es waren weitere, zum Teil erhebliche datenschutzrechtliche Unzulänglichkeiten akkumuliert. So versuchte man, den Datenschutz nach den unzutreffenden Bestimmungen des Bundesdatenschutzgesetzes statt nach Landesrecht zu regeln. Zugriff auf die OWiSch-Datenbank sollten auch das Landesverwaltungsamt und das Ministerium für Wirtschaft und Arbeit erhalten, die, zumindest nach dem SchwarzArbG und der HWO, keine Verfolgungsbehörden für Ordnungswidrigkeiten sind.

Kurz darauf wurde dem Landesbeauftragten bekannt, dass eben diese datenschutzrechtlich unzulängliche Verwaltungsvereinbarung durch das Ministerium für Wirtschaft und Arbeit zum Gegenstand eines Mitzeichnungsverfahrens zum Entwurf einer Kabinettvorlage gemacht worden war. Darin musste er nicht nur lesen, dass das Vorhaben mit dem auch für Datenschutz zuständigen Ministerium des Innern abgestimmt sei, sondern auch, dass „der Landesbeauftragte für den Datenschutz […] gegen eine gemeinsame Nutzung der Datenbank keine Bedenken“ habe. Das war unvollständig, verkannte es doch, dass der Landesbeauftragte gegen verschiedene Verfahrenseinzelheiten erhebliche datenschutzrechtliche Bedenken erhoben hatte und das Gesamtverfahren wegen bisher unterbliebener Vorlage aussagekräftiger Unterlagen überhaupt nicht umfassend prüfbar gewesen war.
Das Ministerium des Innern reagierte im Mitzeichnungsverfahren prompt und konsequent: Es erklärte das Vorhaben, auch wegen bestehender erheblicher datenschutzrechtlicher Bedenken, schlichtweg für „noch nicht kabinettsreif“ und verweigerte die Mitzeichnung. Es wies in seiner Stellungnahme auf die Einwände des Landesbeauftragten hin und empfahl dem Ministerium für Wirtschaft und Arbeit, dem Landesbeauftragten Gelegenheit zur Stellungnahme zum Entwurf der Verwaltungsvereinbarung zu geben. Ein entsprechendes Gesprächsangebot des Landesbeauftragten gegenüber dem Ministerium für Wirtschaft und Arbeit ist kurz vor dem Ende des aktuellen Berichtszeitraumes angenommen worden. Dabei konnte z. B. geklärt werden, dass anhängige Bußgeldverfahren – natürlich als solche gekennzeichnet – wegen sonst möglichen Strafklageverbrauches gespeichert werden sollten. Eine Fülle anderer Fragen blieb dagegen offen. Der Landesbeauftragte wird

die Angelegenheit weiter verfolgen und ggf. im XI. Tätigkeitsbericht erneut zu OWiSch berichten.

13.3 Datenübermittlung vom Finanzamt an die IHK unzulässig?

Ein Gewerbetreibender hatte festgestellt, dass das für ihn zuständige Finanzamt Angaben über die Umsätze und Erlöse seines Gewerbebetriebes an die Industrie- und Handelskammer übermittelt hatte. Er teilte dies dem Landesbeauftragten mit der Bitte um Überprüfung, ob das Rechtens sei, mit.

Die Bedenken des Bürgers konnte der Landesbeauftragte schnell zerstreuen, die Rechtslage ist eindeutig. Die von dem Bürger beobachtete Datenübermittlung ist vom Gesetz sogar so vorgesehen. Das Finanzamt als Daten übermittelnde Stelle erfüllt eine gesetzliche Verpflichtung. In der AO heißt es in § 31 Abs. 1: „Die Finanzbehörden sind verpflichtet, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts [also z. B. die Industrie- und Handelskammer] […] zur Festsetzung solcher Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermessbeträge oder Steuerbeträge anknüpfen."
Genau das hatte das Finanzamt getan, wobei unter Besteuerungsgrundlagen zunächst alle Angaben zu verstehen sind, an welche die Besteuerung anknüpft, nämlich Einkommen, bestimmte Einkunftsarten und die Höhe dieser Einkünfte, Gewinn, Ertrag, Vermögensangelegenheiten und ihr Wert, Umsatz, Gewerbeertrag, Gewerbekapital u. ä. Das Finanzamt darf dabei der Industrie- und Handelskammer jedoch bei weitem nicht alles über die Gewerbetreibenden mitteilen. § 31 Abs. 1 Satz 1 AO bestimmt nämlich, dass die Finanzbehörden den Kammern zwar auf Ersuchen Namen und Anschriften ihrer Mitglieder, die zur Entrichtung von Abgaben verpflichtet sind, und die festgesetzten Abgaben zu übermitteln haben. Es gilt jedoch die Einschränkung, dass diese Daten zur Erfüllung von in der Zuständigkeit der Kammer liegenden Aufgaben, also zur Beitragsfestsetzung, erforderlich sein müssen. So wie die AO für die Finanzverwaltung eine Pflicht zur Datenübermittlung an die Kammern vorgesehen hat, so hat das „Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern" - kurz IHK-Gesetz genannt - eine damit kommunizierende Befugnis zur Erhebung genau dieser Daten durch die IHK bei der Finanzverwaltung vorgesehen. In § 9 Abs. 2 des IHK-Gesetzes heißt es nämlich: „Die Industrie- und Handelskammern […] sind berechtigt, zur Feststellung der Kammerzugehörigkeit und zur Festsetzung der Beiträge der Kammerzugehörigen Angaben zur Gewerbesteuerveranlagung, wie sie auch zur Feststellung der Kammerzugehörigkeit im Sinne von § 2 Abs. 1 IHK-G erforderlich sind, sowie die nach § 3 Abs. 3 IHK-G erforderlichen Bemessungsgrundlagen bei den Finanzbehörden zu erheben."

Damit wird deutlich, dass der Bundesgesetzgeber die Absicht hatte, die Industrie- und Handelskammern in den Stand zu setzen, aufgrund der von den Finanzämtern übermittelten Angaben die aus Grundbetrag und Umlagen bestehenden Beiträge für ihre Mitglieder verbindlich und an der wirtschaftlichen Leistungsfähigkeit der Mitglieder ausgerichtet festzusetzen.
Zu beachten ist jedoch, dass dies alles nur dann gilt, wenn der Betroffene tatsächlich Mitglied einer Kammer ist oder seine Kammerzugehörigkeit festgestellt werden soll.

13.4 Begehrlichkeiten nach bestimmten Gewerbeanzeigen

Wer den selbständigen Betrieb eines stehenden Gewerbes anfängt, muss dies, so § 14 Abs. 1 GewO, der zuständigen Behörde gleichzeitig anzeigen. Nach Nr. 1.1 des Verzeichnisses der Maßnahmen zu Anlage 1 der Verordnung über die Regelung von Zuständigkeiten im Immissions-, Gewerbe- und Arbeitsschutzrecht sowie in anderen Rechtsgebieten (ZustVO GewAIR) sind für die Entgegennahme dieser Anzeigen, die Gewerbeanzeigen genannt werden, die Gemeinden zuständig. Die Anmeldung des Gewerbes hat entsprechend eines Vordruckes zu erfolgen, der sich als Anlage 1 in der GewO findet. Mit dieser Gewerbeanzeige wird eine Fülle von personenbezogenen Daten erhoben, z. B. Name und Anschrift des Gewerbetreibenden, sein Geburtsdatum und sein Geburtsort, seine Staatsangehörigkeit und natürlich eine Fülle von Angaben zu seinem Gewerbebetrieb.

Außer dass die Gemeinden durch die Gewerbeanzeigen erfahren sollen, wer wo welches Gewerbe betreibt und damit ihren Überwachungspflichten nachkommen können, haben sie gemäß § 14 Abs. 9 GewO regelmäßig einer Reihe von Stellen Daten aus den Gewerbeanzeigen zu übermitteln. Da sind die Industrie- und Handelskammern (§ 14 Abs. 9 Nr. 1 GewO) genannt, die für den Immissionsschutz (Nr. 3) und den Arbeitsschutz (Nr. 3a) zuständigen Landesbehörden, die Bundesagentur für Arbeit (Nr. 5), die Zollverwaltung (Nr. 7), das Registergericht (Nr. 8) und neben weiteren Stellen auch die Handwerkskammer (Nr. 2). In allen Fällen hat der Gesetzgeber in § 14 Abs. 9 GewO die Aufgaben und Zwecke bezeichnet, für deren Erfüllung die Daten aus den Gewerbeanzeigen an diese Stellen übermittelt werden dürfen (Zweckbindung). Für die Handwerkskammer beispielsweise sind dies die Führung der Handwerksrolle (§ 6 Handwerksordnung - HwO) und des Verzeichnisses der Inhaber von Betrieben eines zulassungsfreien Handwerks oder handwerksähnlicher Betriebe (§ 19 HwO), der Lehrlingsrolle (§ 28 HwO) und zur Erfüllung der in § 91 HwO genannten weiteren Aufgaben.

In diesem Sinne, so teilte eine Handwerkskammer dem Landesbeauftragten mit, wollte eine Handwerksinnung verfahren. Sie begehrte von der Kammer Kopien solcher Gewerbeanzeigen, die auf die Ausübung zulassungspflichtiger Tätigkeiten eines bestimmten Handwerks zielten. Die Innung wollte, so habe sie der Kammer angegeben, durch Vergleich der Gewerbeanzeigen mit den Eintragungen in der Handwerksrolle und nach Vor-Ort-Kontrollen bei den Gewerbetreibenden Schwarzarbeit aufdecken. Die Kammer hatte das Übermittlungsersuchen der Innung geprüft und erhob, da weder die GewO noch die HwO ihr erlaubten, die Gewerbeanzeigen weiterzugeben, schwerwiegende datenschutzrechtliche Bedenken. Der Landesbeauftragte, von der Kammer um Mitteilung seines Standpunktes gebeten, teilte diese Bedenken, da in der Tat ein Rechtsanspruch der Innung auf Übermittlung der Gewerbeanzeigen nicht bestand und begründete dies wie folgt:

Rechtsgrundlagen für die Übermittlung von Daten im Einzelfall aus der Handwerksrolle bzw. aus den Gewerbeanzeigen an sonstige öffentliche Stellen wie eine Handwerksinnung sind § 6 Abs. 3 HwO bzw. § 14 Abs. 7 GewO. Grundsätzlich gilt jedoch, dass – wie es in § 6 Abs. 3 HwO heißt – öffentlichen Stellen nur solche Daten aus der Handwerksrolle zweckgebunden übermittelt werden dürfen, deren Kenntnis zur Erfüllung der Aufgaben der öf-

fentlichen Stelle als Empfänger erforderlich ist.
Die bei der Kammer die Datenübermittlung begehrende Innung hatte ihr Übermittlungsersuchen mit der möglichen Aufdeckung von Schwarzarbeit begründet. Selbst wenn der Innung diese Aufgabe aus § 54 Abs. 4 HwO erwachsen sein sollte, was der Landesbeauftragte nicht geprüft hat, rechtfertigt das nicht die Übermittlung sämtlicher Daten der einschlägigen Gewerbeanzeigen, sondern nur der für die Erfüllung dieser Aufgabe tatsächlich erforderlichen. Begehrte die Innung mehr als die nach § 14 Abs. 6 GewO öffentlich zugänglichen Grunddaten (Name, Firma, Ort der Niederlassung und betriebenes Handwerk, vgl. IX. Tätigkeitsbericht, Nr. 13.2), bedürfte das der besonderen und nachprüfbaren Begründung.
Im Übrigen kam der Landesbeauftragte auch nach der Prüfung, ob evtl. § 73 HwO (Beiträge und Gebühren der Innungen) als Rechtsgrundlage der Datenübermittlung dienen könnte, zu dem gleichen Ergebnis und bat die Kammer, der Innung auch dies mitzuteilen.

14 Hinweise zum technischen und organisatorischen Datenschutz

14.1 Cloud Computing und Datenschutz

Cloud Computing bedeutet wörtlich übersetzt „Rechnen in der Wolke“ und meint die Nutzung von Soft- und Hardware über ein Netzwerk (häufig das Internet) derart, dass die Parameter, wie zu nutzender Speicher, Rechenleistung oder Festplattenplatz, dynamisch an den Bedarf angepasst werden können. Für Nutzer soll der Betrieb kostengünstiger erfolgen, Anbieter können dadurch Ressourcen und Kosten sparen, indem IT-Systeme für mehrere Nutzer gemeinsam „in der Wolke“, also einer Ansammlung von Servern irgendwo im Netzwerk, betrieben werden. Durch die einheitliche Dienste- und Ressourcen-Bereitstellung können diese wartungsarm und kostengünstig angeboten werden. Das kann dem Datenschutz und der Datensicherheit zugutekommen, muss es jedoch nicht. Bislang überwiegen hier die kritischen Töne, wenn es um den Nachweis von Datenschutz und Datensicherheit in der Cloud geht.

Das grundsätzliche Problem beim Cloud Computing ist die häufig unklare Datenverarbeitung, d. h. es gibt keine Georeferenzierung mehr, wo eigentlich die Datenverarbeitung stattfindet. Irgendwo in der Cloud werden Daten der Nutzer verarbeitet und abgelegt. Da einzelne Teile der Cloud dynamisch zugeteilt werden und Rechner virtuell und somit austauschbar sind, ist es weder garantiert, dass die Daten auf einem bestimmten Rechner bearbeitet werden, noch dass sie nicht den Rechtsrahmen verlassen haben und sich gerade in einem anderen Land mit anderen Datenschutzstandards befinden. Auch die korrekte Datenlöschung kann nicht kontrolliert oder eine gemeinsame Nutzung mit nicht vertrauenswürdigen Dritten ausgeschlossen werden. Mehr noch, es ist möglich, dass ein Auftragnehmer Cloud Computing nutzt, um beispielsweise einen Webserver zu betreiben und so völlig unbemerkt vom Auftraggeber die Daten in einer Cloud verarbeitet werden.

Beim Cloud Computing können verschiedene Ressourcen aufgeteilt und dem Nutzer für diesen bedarfsgerecht verkauft werden. Dies wird durch Nutzung von Virtualisierungstechnologien möglich, welche es erlauben, einzelnen virtuellen Maschinen ihre jeweiligen Ressourcen automatisiert bzw. auf Anfor-

derung, z. B. über eine Webschnittstelle, zuzuteilen. Folgende Dienstarten können in einer Cloud bereitgestellt werden:

- Infrastrukturen: Bei „Infrastructure as a Service“ (IaaS) erhält der Nutzer Zugriff auf eine Infrastruktur, welche er selbst betreuen muss. So wird beispielsweise ein Rechner angeboten, dessen Speichermenge, Netzwerkbandbreite, Festplattenplatz, Geschwindigkeit und Anzahl der Prozessoren konfigurierbar sind. Der Nutzer ist für die Wartung des Betriebssystems selbst verantwortlich. Der Anbieter kümmert sich um die Verfügbarkeit der Ressourcen und hat häufig nichts mit den Daten des Nutzers zu tun. Deshalb sollte dieser auch auf die Verfügbarkeit (Backups, Auslastung) des Dienstes achten. Beispiele dafür sind Amazons Elastic Compute Cloud (EC2) oder typische virtuelle Root-Server großer Anbieter.

- Anwendungen: Bei „Software as a Service“ (SaaS) stellt der Anbieter den Zugriff auf eine Anwendung bereit. Der Nutzer hat mit der zugrundeliegenden Technologie, der Hardware oder der Wartung nichts zu tun und nutzt nur die Datenverarbeitungsmöglichkeiten der Software. Ein typisches Beispiel ist „Google Mail“.

- Plattformen: Bei „Platform as a Service“ (PaaS) erhält der Nutzer eine Infrastruktur mit installierter Programmierschnittstelle (API) und den zugehörigen Werkzeugen. So ist es möglich, eigene Anwendungen in einer Cloud-Umgebung zu schaffen, welche die jeweiligen Vorteile dieser über API-Zugriffe nutzen. Beispiele sind Microsofts Azure oder Googles AppEngine.

Clouds können anhand ihrer Organisationsform wie folgt unterteilt werden:

- „Public Clouds“ sind öffentliche Wolken, deren Nutzer beliebige Personen oder Firmen sein können. Aufgrund der verschiedenen Anforderungen der Nutzer ist der Anbieter gezwungen, exakte und restriktive Regelungen zu Verfügbarkeit und Art und Weise der Nutzung der Dienste vorzugeben. Es kann allerdings passieren, dass sich Anwendungen mit völlig verschiedenen Datenschutz- und Sicherheitsanforderungen gemeinsame Ressourcen teilen. Bedenken entstehen aufgrund der nicht zu gewährleistenden absoluten Datensicherheit, sodass jeder Nutzer genau überlegen sollte, welche Daten in der Wolke verarbeitet werden sollen. Öffentliche Stellen könnten in einer Cloud beispielsweise Webangebote ohne personenbezogene Daten bereitstellen.

- „Private Clouds“ sind private Wolken, deren Merkmal es ist, dass sich Anbieter und Nutzer nicht nur kennen, sondern sich sogar in derselben Organisation befinden, und die Ressourcen dem Nutzer exklusiv zur Verfügung gestellt werden. Nur mit Private Clouds können Datenschutz und Datensicherheit derzeit hinreichend gewährleistet werden.

- Zusätzlich gibt es die Mischform „Hybrid Cloud“. Eine solche liegt dann vor, wenn die Daten einer Stelle in verschiedenen der vorgenannten Wolkenarten verarbeitet werden (können). Häufig anzutreffen

sind Private Clouds, welche bei Bedarf (Lastspitzen oder Ausfälle) Ressourcen aus einer Public Cloud beziehen.

Für die Verarbeitung personenbezogener Daten öffentlicher Stellen kommt in der Regel nur eine „Private Cloud“ in Frage, da in öffentlichen Wolken keine Kontrolle und Einflussnahme des Datenbesitzers möglich ist. Die Nutzung von Hybriden bzw. Public Clouds ist logischerweise dann erlaubt, wenn keine personenbezogenen Daten im Spiel sind.

Wollen öffentliche Stellen personenbezogene Daten im Rahmen des Cloud Computing verarbeiten lassen, ist das DSG-LSA einzuhalten. Cloud Computing ist eine klassische Auftragsdatenverarbeitung (§ 8 DSG-LSA). Die Verantwortung für die verarbeiteten Daten und insbesondere die sorgfältige Auswahl des Auftragnehmers liegt immer beim Auftraggeber, also der öffentlichen Stelle. Vor allem grenzüberschreitende Datenflüsse wie beispielsweise außerhalb der EU sind rechtlich problematisch und derzeit unbedingt zu vermeiden (siehe § 2 Abs. 9 Satz 2 DSG-LSA). Für öffentliche Stellen kommt Cloud Computing insbesondere im Rahmen der Nutzung in landeseigenen Rechenzentren in Frage. Bei Angeboten privater Unternehmen muss der Anbieter und insbesondere seine IT-Infrastruktur vor Auftragserteilung genau betrachtet werden. Das ist in den meisten Fällen für die öffentlichen Stellen als Verantwortliche der Datenverarbeitung nicht möglich. Weiterhin muss sich der private Cloud-Anbieter der Kontrolle durch den Landesbeauftragten unterwerfen. Inwieweit dabei die Schutzziele des § 6 DSG-LSA umgesetzt und kontrolliert werden können, ist fraglich.

Gegenwärtig fehlen konkrete rechtliche Regelungen und technische Normen für sicheres Cloud Computing. Diese Rechtsunsicherheit gilt es auszuräumen. Das Bundesamt für Sicherheit in der Informationstechnik hat in einem Eckpunktepapier (https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html) die wesentlichen Minimalanforderungen an Cloud-Service-Anbieter erarbeitet und der Öffentlichkeit zur Diskussion gestellt. Sie geben einen Rahmen für ein Mindestsicherheitsniveau vor, auf welches der Anbieter verpflichtet werden sollte.

Die EU fördert die Entwicklung sogenannter „Trustworthy Clouds“ (TClouds). Diese sollen eine vertrauenswürdige, transparente und sichere Cloud-Computing-Infrastruktur bilden, welche nach EU-Recht legal und datenschutzgerecht zur Datenverarbeitung genutzt werden kann.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK Technik) befasst sich mit diesem aktuellen Thema. Zielstellung des AK Technik ist es, noch im Jahr 2011 die Erarbeitung einer Orientierungshilfe zum Thema „Cloud Computing und Datenschutz“ abzuschließen. Diese wird aus Sicht des Datenschutzes und der Datensicherheit entsprechende Empfehlungen geben. Nach Zustimmung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird diese Orientierungshilfe zeitnah auf den Webseiten des Landesbeauftragten eingestellt werden.

14.2 Löschung von Datenträgern – aktuelle Entwicklung

Das datenschutzgerechte Löschen bzw. Entsorgen von magnetischen Datenträgern (Bänder, Festplatten) ist regelmäßiges Beratungsthema. Aufgrund von Unzulänglichkeiten der vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) angebotenen und bisher auch vom Landesbeauftragten empfohlenen Löschsoftware VS-Clean hat sich der Landesbeauftragte beim BSI nach den aktuellen Weiterentwicklungen und Alternativen erkundigt.

VS-Clean ist eine mit Version 2.1 letztmalig im Jahr 2002 aktualisierte DOS-Anwendung, welche auf veraltete Rechner zugeschnitten ist und für neuere PC- und Speichertechnik nicht mehr nutzbar ist. Eine Überarbeitung ist seitens des BSI nicht mehr vorgesehen. Diese Löschsoftware wird vom BSI selbst als nicht mehr zeitgemäß angesehen. In einem Hinweisblatt (Stand 15. Juni 2011) weist das BSI auf die Anforderungen an Software zum Löschen von Festplatten ausdrücklich hin.

Häufig erlauben es moderne Festplatten mittels „Host Protected Area“ (HPA) oder „Device Configuration Overlay“ (DCO), den Bereich, auf den zugegriffen werden darf, einzuschränken. Derartige Beschränkungen müssen vor der Löschung beachtet und aufgehoben werden. Auch können „bad blocks“, also Datenbereiche, die defekt sind oder bald defekt werden könnten und nicht mehr verwendet werden, von Software nicht ohne Weiteres direkt angesprochen und somit auch nicht restlos gelöscht werden. Das ist auch der Grund, warum Datenträger mit hohen Sicherheitsanforderungen entmagnetisiert (mittels Degausser) oder physisch vernichtet (Zerkleinerung durch Schreddern) werden sollen.

Zum Überschreiben magnetischer Datenträger ist derzeit VS-Clean für „VS-NfD“ und „VS-Vertraulich“ unter Beachtung der gegebenen Hinweise des BSI noch zugelassen. Es werden jedoch die Produkte DBAN/EBAN (DBAN ist eine kostenfreie Open Source Software, http://www.dban.org) und Blancco Erasure (Firma Blancco) für „VS-NfD“ durch das BSI empfohlen. Für letztere Software wird eine erfolgreiche Zertifizierung des Produkts durch das BSI in naher Zukunft erwartet.

Ganz andere Löschanforderungen bestehen bei Flash-Speichern, also z. B. Solid State Drives (SSD), USB-Sticks oder Speicherkarten. Diese speichern ihre Inhalte in Form von elektrischen Ladungen in Speicherzellen. Diese sind elektrisch nahezu isoliert, jedoch kann die Unzugänglichkeit der Zelle für Ladungen mit hohem Energieaufwand überwunden werden. Zum Auslesen wird der Effekt genutzt, dass der Ladezustand der Speicherzelle Einfluss auf einen benachbarten Transportweg für elektrische Ladungen nehmen und dessen Durchlassfähigkeit manipulieren kann. Um sicher löschen zu können, muss die Speicherzelle also nur auf einen konkreten Wert gesetzt werden. Leider weisen diese Speicherzellen eine begrenzte Haltbarkeit auf. Damit ist es erforderlich, häufig genutzte Zellen ggf. vorbeugend zu deaktivieren und besser Reservezellen zu nutzen. Diese Speicherbereiche (Stichworte: Wear Leveling, Flash Translation Layer) sind nur für die Elektronik des Mediums zugreifbar und können nicht gezielt gelöscht werden, da die Adressierung auf Sektorebene der ATA-Schnittstelle für Festplatten gedacht war und für Flash-Chips diese auf eine andere Adressierungsform und andere Chip-Bereiche

umgesetzt werden muss. Auch dauert das Löschen deutlich länger als das Auslesen der Daten, sodass bei Datentransfers auf Flash-Speicher häufig nicht gelöscht, sondern nur das Inhaltsverzeichnis der freien Bereiche aktualisiert wird. Und selbst, wenn gelöscht werden könnte, verfügt jeder Hersteller über eigene Methoden des Zugriffs, sodass der tatsächliche Datenspeicherort, der gelöscht werden soll, jeweils verschieden zu ermitteln ist. Hier fehlen einheitliche Vorgaben und Standards.

SSDs, also Festplatten mit Flash-Chips oder völlig auf Flash-Basis, bieten zwar oft den Befehl „ATA Secure Erase“ zum sicheren Löschen an, dieser ist teilweise jedoch nicht korrekt implementiert oder eben gar nicht vorhanden. Derzeit müssen Flash-Speicherchips auf physischer Ebene, z. B. thermisch, vernichtet werden, um nicht versehentlich sensible Daten weiterzugeben.

Sicher genutzt werden können Flash-basierte Technologien auch unter Verwendung einer als sicher bekannten Verschlüsselungstechnologie (z. B. TrueCrypt), da dann das einfache Löschen der Zugriffsschlüssel aus den Daten für einen unbefugten Benutzer Zufallszahlen macht. Viele PCs können auch im BIOS – ggf. mit Software des Herstellers – mit einem Passwort zum Verschlüsseln der angeschlossenen Datenträger versehen werden oder ein vorhandenes Trusted Platform Module (TPM) des PCs dafür nutzen. Eine Verschlüsselung ist Stand der Technik und muss, ggf. mit begründeten Ausnahmen, für alle personenbezogenen Daten grundsätzlich gezielt genutzt werden.

Eine deshalb notwendige Aktualisierung der Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz aus dem Jahr 2004 steht noch aus, wurde aber bereits begonnen.

14.3 Mobile Computing und Datenschutz (vom iPhone bis zum BlackBerry)

Der Ausdruck „Mobile Computing“ kennzeichnet die Nutzung mobiler Endgeräte, welche schon seit langem die Rechenleistung und Komplexität von PCs erreicht haben und damit in den Möglichkeiten aktuellen PCs in nichts mehr nachstehen. In der Regel sind damit Smartphones gemeint, also Mobiltelefone, welche beliebige Anwendungen ausführen können und aufgrund ihrer flexiblen Möglichkeiten sehr beliebt sind. Mit der stetig steigenden Funktionalität, der hohen Verbreitung und immer einfacher werdenden Nutzbarkeit steigt auch die Nachfrage im öffentlichen Sektor, sodass dem Datenschutz und der Datensicherheit Rechnung getragen werden muss.

Smartphones und mobile Computer sind nur deshalb flexibel einsetzbar, weil sie mit dem Internet vernetzt werden können und einfachen Zugriff auf Internetdienste wie Webseiten, E-Mails und Soziale Netzwerke haben. Dies wird unterstützt durch aktuelle Funktechnologien GSM, UMTS und LTE und die zunehmende Verbreitung und Akzeptanz von WLAN und Bluetooth. Zusätzlich sind unzählige Sensoren enthalten, welche die aktuelle Position, Zeit, Geschwindigkeit, Neigungen, Höhenangaben, Bildinformationen (Kamera) und Temperatur selbständig ermitteln und Anwendungen zur automatisierten Weiterverarbeitung zur Verfügung stellen.

Eine Nutzung von Smartphones ohne Angabe personenbezogener Daten ist zurzeit nur eingeschränkt möglich. Auch personenbezogene Daten Dritter werden erfasst und alle im Telefon gespeicherten Daten werden weitgehend unkontrollierbar überall hin verteilt. So sind beispielsweise die Kontaktdaten sehr schnell für andere Anwendungen zugänglich, da viele Anwendungen dies erzwingen und sonst nicht sinnvoll nutzbar wären. Andere Anwendungen erzwingen einen weitgehenden Zugriff auf die Nutzerdaten und Rechte, indem personenbezogene Daten des Nutzers, welche von Dritten angelegt wurden, erst angezeigt werden, wenn alle Rechte gewährt wurden. Diese werden dann ggf. genutzt, um die Anwendung „viral“ im Freundeskreis weiter zu verbreiten.

Die Shop-Systeme der Plattform-Betreiber sind mittelfristig zu modernisieren, und es sind Datenschutzstandards zu schaffen, die diesen Namen auch verdienen. Eine Beschränkung der Möglichkeiten einer Anwendung auf minimale Rechte und Datenfreigaben ist sinnvoll. Es sollte ggf. ein Impressum existieren, sodass der Urheber ermittelbar ist. Zu jedem Anbieter sollten die Meinungen der anderen Nutzer direkte Auswirkung auf die Verfügbarkeit der Anwendung im Online-Markt haben. Ab einer bestimmten (schlechten) Durchschnittsmeinung sollten Anwendungen z. B. nur nach einem Warnhinweis installiert werden können.

Die auf den Geräten laufenden Anwendungen erhalten Zugriff auf von diesen bestimmte Sensoren, Daten und Kommunikations-Arten wie die Kontakte, die E-Mails, SMS oder das Internet selbst. Damit können unbemerkt Daten zum Hersteller der Anwendung übertragen werden. Das ist bereits eine gängige Praxis. Hier müssen die Anbieter unbedingt nachbessern. Beispielsweise könnte eine kurze Begründung zu den einzelnen Zugriffsanforderungen erfragt werden, eine detaillierte Datenverwendungsbeschreibung ggf. sogar mit standardisierten Vorgaben verlinkt werden. Anwendungen sollten auch funktionieren, wenn einige oder alle der gewünschten Zugriffe nicht gewährt werden können oder sollen.

Des Weiteren sind viele Smartphones an den Hersteller bzw. spezielle Diensteanbieter gekoppelt. Das geschieht oft per Voreinstellung oder zwangsweise. So gehört die weit verbreitete Android-Plattform (38,5% Marktanteil [Studie vom April 2011, http://www.gartner.com/it/page.jsp?id =1622614], steigend) zu Google und möchte natürlich über einen Google-Account Dienste wie Google Mail, Google Maps oder Google Talk nutzen. Windows Mobile (5,6%, steigend) gehört zu Microsoft und bindet sich an das Live-Netzwerk desselben Herstellers, BlackBerrys (13,4%) kommunizieren über Server des Herstellers RIM und auch Apple (19,4%) will die Kontrolle über die Nutzerdaten von iPhone-Nutzern behalten. Einwilligungen in die Nutzung personenbezogener Daten werden dem Nutzer oft abgezwungen. Hinzu kommt, dass über Anwendungen auch alle diese Dienste parallel genutzt werden können, sodass ein Microsoft Messenger z. B. auch via Android-Handy nutzbar ist. Daten aus den verschiedenen Sozialen Netzwerken sind entweder direkt zugreifbar (sodass z. B. die Daten der Freunde des Netzwerks heruntergeladen werden und direkt in den Kontakten des Handys erscheinen) oder per zusätzlich zu installierender Anwendung (Twitter, Facebook, XING, …) zugänglich. Damit werden sowohl eigene als auch fremde personenbezogene Daten in der ganzen Welt verteilt und der Nutzer hat häu-

fig keine Kontrolle und keinen Überblick mehr darüber, welche Daten wohin übertragen werden.

Sehr kritisch zu betrachten sind die Anwendungen (sog. Apps) auf den Geräten. Diese informieren zur Installation über die benötigten Zugriffsrechte und Ressourcen, jedoch gibt es systembedingt oft keine Möglichkeit, diese zu verweigern. Wer sich z. B. fragt, wozu ein Notizbuch Internetzugriff benötigt oder warum ein Wörterbuch SMS verschicken können soll, der erhält meist nur eine kurze Standard-Information. Der Zugriff kann nur blockiert werden, indem die Anwendung nicht installiert wird. Der Normalnutzer wird die Information nicht einmal zur Kenntnis nehmen bzw. sich auf die Nutzerbewertung („so viele Prozent der Herunterlader finden die Anwendung gut“) verlassen, die allerdings keine Aussage zur Datensicherheit trifft. Danach muss dem Hersteller der Anwendung vertraut werden, der jedoch in der Regel gewinnorientiert arbeitet und deshalb häufig Daten sammeln wird. Oft ist dieser nicht einmal eindeutig bestimmbar.

Smartphones müssen sicher und datenschutzgerecht betrieben werden können. Smartphone-Hersteller müssen ihre Geräte derart nachbessern, dass die Zugriffsrechte von Anwendungen einzeln und detailliert konfigurierbar sind und dass über Datenflüsse (vorab) informiert wird, damit Berechtigungen und Risiken für den Anwender oder Administrator transparent werden und gezielt beeinflusst werden können. Eine Nutzung ohne Übertragung personenbezogener Daten zum Hersteller des Geräts muss möglich sein. Bei Bedarf können zusätzliche Rechte durch Einwilligung vor der Übertragung gegeben werden. Alle Datenübertragungen zum und Datenspeicherungen auf dem Gerät sind verschlüsselt vorzunehmen. Zugriffe Dritter (Telefonhersteller, Netzbetreiber, Diensteanbieter, Anwendungshersteller) auf Übertragungen personenbezogener Daten sind durch Ende-zu-Ende-Verschlüsselung oder gleichwertige Datenschutz-Maßnahmen nach dem Stand der Technik zu unterbinden. Sicherheitsrelevante Algorithmen sind offenzulegen und müssen von einer unabhängigen und vertrauenswürdigen Stelle als sicher anerkannt und ebenso implementiert worden sein. Gefundene Fehler müssen durch Aktualisierungen von Betriebssystem und Anwendungen bei den Nutzern zügig ausgebessert werden. Insbesondere die IPv6-Unterstützung, die Fernadministration und die VPN-Unterstützung der Geräte bzw. Anwendungen sind häufig verbesserungsfähig.

Der Einsatz solcher mobilen Endgeräte im Bereich der öffentlichen Verwaltung bedarf deshalb einer vorherigen Risikoanalyse und der Umsetzung konkreter Schutzmaßnahmen, um zu verhindern, dass bei der Einbindung solcher Technik in lokale Netze die Sicherheit aller angeschlossenen Systeme beeinträchtigt wird.

14.4 Datenschutz durch Einsatz von IPv6

Computer im Internet erkennen sich und kommunizieren untereinander unter Nutzung von eindeutigen Nummern, sogenannten IP-Adressen. Die bisher verwendeten Nummern bestehen aus 4 jeweils 8 Bit großen Zahlen (32 Bit), beispielsweise „129.92.121.153“. Die darüber ansprechbare Menge an Computern ist allerdings begrenzt (ca. 4 Mrd.), das Netz ist an seine Grenzen gestoßen und kann nicht mehr weiter wachsen. Bereits seit 15 Jahren wird eine

größere Adresse propagiert, welche auch funktionieren wird, wenn das Internet größer wird und mehr Geräte adressiert werden müssen. Dieses Internetprotokoll Version 6 (IPv6) wurde in der letzten Zeit häufig in der Fachpresse kritisch hinterfragt. Die Einführung des neuen Standards IPv6 für größere IP-Adressen (128 Bit) wirft derzeit viele Fragen bzgl. der datenschutzgerechten Umsetzung auf. Eine neue Technologie darf aber nicht allein deshalb verhindert werden, nur weil sie bei falscher Anwendung eine Gefahr darstellen könnte. Vielmehr muss bereits im Vorfeld eine Lösung gefunden werden, wie die Rahmenbedingungen aussehen müssen, um IPv6 datenschutzgerecht einsetzen zu können. Inwieweit der Datenschutz und die Sicherheit gerade durch IPv6 verbessert werden könnten, ist gegenwärtig noch nicht abschließend beurteilbar. Im Folgenden wird eine Zusammenfassung der aktuellen Erkenntnisse und Empfehlungen gegeben.

Eine häufig anzutreffende Meinung ist, dass bei Nutzung von IPv6 automatisch auf den Datenschutz verzichtet werde, da durch die im Überfluss zur Verfügung stehenden IP-Adressen diese nun bevorzugt statisch vergeben werden würden und so der Profilbildung über eine Person Tür und Tor geöffnet werden würde. Das ist derzeit nicht zu erwarten, da die Telekommunikations-Anbieter zur Vermeidung des Betriebs von Server-Diensten auf statischen Nummern diese regelmäßig trennen und die IP-Adresse neu vergeben. Der Versuch von Profilbildungen ist jedoch verstärkt zu erwarten.

Die Nutzung von IPv6 kann auch dem Datenschutz dienen, da es die derzeit vorhandenen, auf NAT-basierenden Netzwerke mit eigenen Sub-Netzwerken erforderlich machen, zur direkten Kommunikation zwischen Endgeräten vermittelnde Server der Anbieter zu nutzen. Um beispielsweise ein Voice over IP (VoIP)-Telefonat zwischen zwei Teilnehmern, welche hinter einem NAT liegen, zu führen, ist es notwendig, die Firewall zu durchtunneln, was oft nicht möglich ist, oder den Verkehr über einen vertrauenswürdigen Dritten zu leiten. Das ist in der Regel der Hersteller der jeweiligen Software und dieser ist in den wenigsten Fällen absolut vertrauenswürdig. Dieser Dritte kann nicht nur den Datenverkehr mitlesen, sondern auch Kommunikationsprofile der Teilnehmer erstellen. Mit IPv6 wird es möglich, dass Endgeräte wieder direkt miteinander kommunizieren (Peer-to-peer-Prinzip), was derartige Profilbildungen verhindert, da die Daten nicht mehr zentral abgegriffen werden können. Das ist ein großer Fortschritt und wird sogar die Programmierung von Software erleichtern. Zentrale Server sind Dreh- und Angelpunkt in den gegenwärtig IPv4-basierten Netzwerken und ermöglichen Angriffe auf die jeweilige Technik.

Ein weiterer Nachteil von NAT ist es, dass Verschlüsselungen nicht Ende-zu-Ende funktionieren, sondern getunnelt werden müssen, da die Gegenstelle nicht direkt erreichbar ist. Die Kommunikation ist oft nicht durchgängig verschlüsselt. Es ist sogar vorstellbar, dass gar keine verschlüsselten Verbindungen durch die Firewall kommen und damit oft auch kein Schutz der Kommunikation existiert.

Bedenken der Nutzer bestehen auch hinsichtlich statischer IPv6-Adressen, deren Datenverkehr jederzeit wieder dem gleichen Internetanschluss zugeordnet werden kann. Vorstellbar ist eine Zuordenbarkeit bis auf die Ebene des Endgeräts. Damit könnten unbefugte Dritte gezielt Profile erstellen und

Nutzer überwachen. Aber ist eine statische IPv6-Adresse wirklich weltweit eindeutig? Eine IPv6-Adresse besteht aus zwei Teilen, einem Präfix, der vom Internetanbieter zugewiesen wird und einem Anschluss zugeordnet ist, und einen Interface Identifier, der vom Kunden des Anbieters völlig frei für jedes einzelne Endgerät gewählt werden kann. Beide Teile der 128 Bit langen Internet-Adresse können weltweit eindeutig sein. Beide können der Ermittlung des Teilnehmers dienen und müssen sich daher regelmäßig ändern. Der Interface Identifier muss zufällig genug gewählt werden, dass er nicht leicht erraten werden kann und sich doch der Rechner in der Menge der Möglichkeiten so verstecken kann, dass er bei einem Absuchen von Adressbereichen nicht gefunden wird. Ein komplettes Scannen aller 2^{64} Möglichkeiten (18,4 Trillionen) ist im Gegensatz zu IPv4 (mit ca. 4 Mrd. IP-Adressen) nicht einfach möglich. Leider wird der Interface Identifier oft aus der Adresse der Hardware der Netzwerkschnittstelle (MAC-Adresse) abgeleitet und damit immer wieder gleich erzeugt. Hier ist darauf zu achten, dass der Interface Identifier wirklich zufällig ist.

Ziel muss es also sein, IPv6-Netze mindestens mit gleichwertigen Möglichkeiten zur datenschutzgerechten Nutzung zu realisieren, wie das auch schon bei IPv4 mit NAT und dynamisch vergebener IP-Adresse der Fall ist. Das geht mittels sogenannter „Privacy Extensions“. Dabei wird der Interface Identifier regelmäßig geändert und auch die Präfixe des Providers sind dynamisch vergeben (also wie bei IPv4). Ständig andere Präfixe und Interface Identifier sind nicht gut nutzbar. Ständig würde sich die IPv6-Adresse ändern und Verbindungen würden ggf. unnötig unterbrochen werden bzw. es wären lange Tabellen mit noch gültigen alten Adressen zu merken. Statisch geht es aber auch nicht, da die Endgeräte ja nicht nur anhand ihrer IP-Adresse wiedererkannt werden können sollen. Gebraucht werden also möglicherweise sowohl statische als auch dynamische Präfixe zur gleichen Zeit. Das sollte der Internetprovider anbieten und nur so kann der Nutzer sowohl anonym und dynamisch im Netz unterwegs sein als auch für andere Dienste wie Chat oder Telefonie statisch erreichbar sein.

Zum Thema Absicherung von IPv6 gehören zwangsläufig auch die Themen DNS Security Extensions (DNSSEC) und Routing Public Key Infrastructure (RPKI). Mit DNSSEC werden die Namenseinträge zu den IP-Adressen kryptografisch mittels Public-Key-Verfahren gesichert. Dazu werden die den einzelnen Zonen zugeordneten Zonenschlüssel (Zone Signing Keys) des autoritativen Master-Name-Servers mittels Schlüsselunterzeichnungsschlüssel (Key Signing Key), der auch in der darüber liegenden Zone hinterlegt ist, beglaubigt. Somit existieren Vertrauensketten, welche überprüft werden können. Die Zonenschlüssel dienen der Beglaubigung der Resource Records der einzelnen Zonen. Seit Juli 2010 ist der Rootzonenschlüssel veröffentlicht. Mit diesem ist das DNS von der Wurzel an validierbar.

Zusätzlich sollten IPv6-Adressen kryptografisch geschützt werden, sodass die Angaben zum IP-Inhaber nicht mehr gefälscht werden können. Das ist seit Jahresbeginn 2011 mit Hilfe von durch das RIPE NCC (nur in Europa) ausgestellten Zertifikaten der RPKI möglich. Diese Zertifikate gibt es zu IPv6-Adressen auf Wunsch dazu, jedoch können Provider (später) auch selbst als CA derartige Eigentümernachweise (End Entity Certificates) ausstellen. Dann kann der Provider seine Route Origin Authorizations (ROA) unterschreiben

und somit einen Gültigkeitsvermerk des IP-Inhabers bspw. zu Routengültigkeiten und -änderungen anhängen. Derzeit gibt es kein zentrales Wurzelzertifikat, da dieses in den USA (ICANN/IANA) liegen und der dortigen Regierung unterstehen würde.

Auch könnte es passieren, dass mit zunehmender Verbreitung dieser zertifikatsbasierten Schutzmaßnahmen der Druck auf die Nicht-Nutzer steigt. Möglich ist auch, dass große Provider Datenströme unterschiedlich klassifizieren und transportieren oder gar gänzlich sperren.

Der Landesbeauftragte geht davon aus, dass sich das Landesrechenzentrum mit dieser Thematik bereits eingehend befasst und entsprechende Lösungen für das jetzige und das zukünftige Landesnetz erarbeitet werden. Es gibt bereits erste Internetdienste, die nur via IPv6 zugänglich sind. Teilnehmer müssen per IPv6 kommunizieren können und ggf. ihre IT-Infrastruktur an den neuen Standard anpassen können, ohne durch das Landesnetz in ihren Bemühungen gehindert zu werden. Nur so lassen sich noch vorhandene Defizite wie beispielsweise bei Routern o. ä. erkennen.

14.5 Veraltete Software ist kein „Stand der Technik“

Bei Kontrollen in öffentlichen Stellen fallen regelmäßig Computer mit Internet-Zugang, aber ohne aktuelle Software auf. Wenn der Hersteller des Betriebssystems oder einer Anwendung Aktualisierungen kostenfrei bereit stellt, so ist der Anwender bzw. Administrator in der Pflicht, diese auch einzuspielen. Im Zweifel sollte die automatische Update-Funktion der entsprechenden Software aktiviert werden.

Während das Betriebssystem und Anwendungen desselben Herstellers noch relativ einfach aktualisiert werden können, kommen Anwendungen von Drittanbietern jeweils mit eigenen Aktualisierungs- und Installationsroutinen. Das ist nicht zeitgemäß, lässt sich aber durch Microsofts Aktualisierungspolitik erklären. Folgenden Forderungen muss ein modernes Betriebssystem genügen:

- Aktualisierungen müssen zentral eingespielt werden können. Der Betriebssystemhersteller sollte Möglichkeiten für Softwarehersteller anbieten, eigene Patches auf den Standardwegen auszuliefern.

- Der Betrieb von Aktualisierungs-Servern sollte auch auf Arbeitsplatz-PCs möglich sein. Im Idealfall würde eine verteilte Infrastruktur zur Speicherung von Updates usw. genutzt werden können.

- Aktualisierungen müssen möglichst ohne Nachfragen oder Neustarts installiert werden können.

- Aktualisierungen müssen auch bei Nutzung eines eingeschränkten Zugangskontos installiert werden können und dürfen keine Seiteneffekte, z. B. aufgrund fehlender Rechte, haben.

Es ist legitim, alte Software zu nutzen, jedoch bedeutet dies oft auch, den Rechner von potentiell unsicheren Netzwerken wie dem Internet zu trennen.

Es reicht nicht, sich darauf zu verlassen, dass der Router oder die Firewall Zugriffsversuche von außen blockieren werden.

Im Land fehlt ein zentrales Software-Management. Es ist nicht sinnvoll, wenn jede Behörde Standard-Software selbst ausprobieren, testen, in MSI-Archive konvertieren und regelmäßig aktualisieren muss. Es müssen fertige Pakete zentral bereitgestellt werden, welche jeweils die aktuellste getestete Software enthalten und automatisiert installiert und aktualisiert werden können. Selten genutzte Software sollte als portable Installation ebenfalls zentral angeboten werden, sodass eine Behörde nur einen Spiegelserver einrichten muss und ständig jede aktuelle (freie) Software zur Verfügung steht. Nutzer werden durch fehlende und veraltete Software zur Unproduktivität und Unsicherheit gezwungen. Die Weiterbildung in vielen Behörden stagniert, viele Mitarbeiter kommen gar nicht auf die Idee, aktuelle Software zu verlangen und nutzen „was da“ ist. Es ist z. B. nicht zeitgemäß, Fotografien aufwändig mit mspaint.exe (von Windows XP) zu bearbeiten, wenn gleichzeitig sehr gute Alternativen zur Verfügung stehen. Alternativsoftware ist fast immer kostenfrei und ohne Einschränkungen nutzbar. Von der Nutzung von veralteten Internet Explorern wird explizit abgeraten. Der Internet Explorer ist mindestens in der Version 8, nach Möglichkeit in der Version 9 bei Zugriffen auf das Internet einzusetzen. Auch in diesem Fall wird geraten, ggf. alternative Software zu nutzen, welche in der Regel auch ohne tiefgreifende Änderungen am Betriebssystem auskommt und einfach erprobt und betrieben werden kann.

14.6 Datenschutzgerechtes Web-Tracking

Immer mehr Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder zur bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten ihrer Nutzerinnen und Nutzer. Sowohl öffentliche als auch nicht-öffentliche Stellen verwenden dazu meist Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden. Am weitesten verbreitet ist das von der Firma Google kostenlos zur Verfügung gestellte Web-Analysetool Google Analytics.

In einem Beschluss vom 26./27. November 2009 zur „Datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ (**Anlage 24**) haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich darauf hingewiesen, dass bei der Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur unter Verwendung von Pseudonymen erstellt werden, wobei die IP-Adresse kein Pseudonym im Sinne des TMG darstellt.

Gemäß § 15 Abs. 3 TMG ist es Diensteanbietern gestattet, für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung von Pseudonymen zu erstellen, sofern der Nutzer dem nicht widerspricht. Voraussetzung ist, dass die Nutzerinnen und Nutzer der betreffenden Website vor der Erhebung ihrer Nutzungsdaten umfassend über Art, Umfang, Dauer und Verwendung der Erhebung und Speicherung informiert werden und ihnen die Möglichkeit eingeräumt wird, der Erstellung des Nutzungsprofils zu widersprechen.

Des Weiteren dürfte der Diensteanbieter gem. § 12 Abs. 2 TMG für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke verwenden, wenn der Nutzer darin eingewilligt hat.

Da Google Analytics zum damaligen Zeitpunkt weder eine Widerspruchs- noch eine Einwilligungsmöglichkeit bot, wurde die Nutzung dieses Web-Analysetools als unzulässig bewertet. Außerdem war eine wirksame Wahrnehmung des Rechts auf Information und Auskunft sowie Löschung der Daten durch den Betroffenen nicht möglich.

Auch in Sachsen-Anhalt wurde im Rahmen von Kontrollen und bei Stichproben festgestellt, dass bei einer Reihe öffentlicher Stellen vor allem im kommunalen Bereich das Web-Analysetool Google Analytics zum Einsatz kam. Daraufhin forderte der Landesbeauftragte die öffentlichen Stellen auf, ein Web-Analysetool einzusetzen, dass den Anforderungen des TMG Rechnung trägt oder ganz auf eine Webanalyse zu verzichten.

Aufgrund der anhaltenden Kritik aus den Reihen der Datenschutzbeauftragten des Bundes und der Länder sowie der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fanden mehrere Gespräche sowie Schriftwechsel mit der Firma Google Germany GmbH statt. Im Rahmen dieser Kontakte wurden unter anderem Vorschläge zur Kürzung der IP-Adresse und zur Bereitstellung eines Browser-Plugins als Widerspruchsmöglichkeit unterbreitet, die mittlerweile auch umgesetzt wurden.

Hinsichtlich des Browser-Plugins ist festzustellen, dass der Nutzer damit zwar die Möglichkeit erhält, die Ausführung des Google Analytics-Skripts zu unterbinden, allerdings geht dabei die Verantwortung des Telemedien-Anbieters auf den Nutzer über. Außerdem ist dieses Plugin noch nicht für alle Browsertypen verfügbar, sodass einem Teil der Nutzer auch weiterhin keine Möglichkeit des Widerspruchs eingeräumt wird. Dies betrifft insbesondere die Gruppe der Smartphone-Nutzer, da die dort genutzten Browser die Plugin-Technik nur zum Teil unterstützen.

Bei der Kürzung der IP-Adresse um das letzte Oktett blieb die Frage offen, ob die Kürzung vor Weitergabe der Daten in die USA erfolgt oder erst danach. Die Übermittlung der vollständigen IP-Adresse ohne Einwilligung des Nutzers wird weiterhin kritisch bewertet. Außerdem muss davon ausgegangen werden, dass Nutzer auch ohne Verwendung der IP-Adresse hinreichend genau identifiziert werden können, insbesondere dann, wenn sie noch weitere Google-Dienste nutzen und dort registriert sind.

Im Kreis der Datenschutzbeauftragten und Aufsichtsbehörden ist die Meinungsbildung, ob mit den vorgenommenen Veränderungen ein datenschutzkonformer Einsatz von Google Analytics möglich ist, noch nicht abgeschlossen. Der Landesbeauftragte hält die Nutzung dieses Web-Analysetools weiterhin für kritisch und verweist deshalb auf freie Alternativsoftware wie z. B. Piwik. Bei verschiedenen Informations- und Kontrollbesuchen in sachsen-anhaltischen Kommunen wurde festgestellt, dass diese Alternativen mittlerweile auch genutzt werden. Das liegt nicht zuletzt an der weitgehend einheitlichen Betreuung der Internet-Auftritte.

Für Nutzer, die ihre Privatsphäre schützen wollen, sind insbesondere Browser-Erweiterungen zum Ausfiltern und Blockieren von Spionage-Elementen aus Webseiten einfach nutzbar. Empfehlenswert ist z. B. die Erweiterung Ghostery in Verbindung mit dem Browser Firefox. Alternativ kann die NoScript-Erweiterung verwendet werden. Außerdem wird auf die im IX. Tätigkeitsbericht unter Nr. 14.9 gegebenen Empfehlungen verwiesen.

14.7 Sicherheitsleitlinie der Verwaltungs-PKI des BSI – Sachstand

Die Überarbeitung der Sicherheitsleitlinie der Verwaltungs-PKI des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde weiterhin begleitet, worauf in Fortschreibung der Hinweise des IX. Tätigkeitsberichts (Nr. 14.3) kurz eingegangen werden soll. Damals zeichnete sich bereits ein erfolgreiches Ende der Mitwirkung der Datenschützer ab, jedoch stagnierte die Weiterarbeit an der überarbeiteten Sicherheitsleitlinie der Verwaltungs-PKI des BSI Anfang 2010 überraschend. Erwartet wurde eine schnelle Einarbeitung der Empfehlungen der Arbeitsgruppe (AG), zumal auch der Vertreter des BSI keine größeren Meinungsdifferenzen zwischen BSI und AG durchblicken ließ. In den der AG Verwaltungs-PKI zugearbeiteten Dokumenten des BSI, einem überarbeiteten Entwurf der Sicherheitsleitlinien der Wurzelzertifizierungsstelle und auch einem Entwurf der Sicherheitsleitlinien für Zertifizierungsstellen der PKI-1-Verwaltung, welche durch das BSI zur Kommentierung gegeben wurden, fehlten erwartete Aussagen. Damit rückte die Hoffnung auf ein baldiges Ende der Arbeit der AG in die Ferne, da sowohl bereits erfolgte Absprachen und Zusagen nicht enthalten waren als sich auch neue Unzulänglichkeiten offenbarten. Bis zum Ende des Berichtszeitraums erfolgten jedoch keine Treffen mehr, da abgewartet werden sollte, welche der Forderungen sich nach der geplanten Novellierung des Signaturgesetzes (koordiniert durch das Bundesministerium für Wirtschaft und Technologie) in diesem wiederfinden werden und damit ggf. nur referenziert werden müssten.

14.8 Kontaktformular im Landesportal

Im vergangenen Berichtszeitraum hatte der Landesbeauftragte eine datenschutzrechtlich bedenkliche Entwicklung im Zusammenhang mit dem Landesportal http://www.sachsen-anhalt.de zu konstatieren und im IX. Tätigkeitsbericht (Nr. 2.5) auch bereits darüber berichtet. Es ging um das Service-Icon „Briefumschlag“ unter dem Hauptmenü auf fast jeder Seite im Landesportal, durch dessen Anklicken mittels eines Kontaktformulars eine E-Mail an die Onlineredaktion gesandt werden konnte. Dutzende Nutzer hatten geglaubt, in Kontakt mit der Onlineredaktion eines Ministeriums, eines Finanzamtes oder des Landesbeauftragten zu treten und offenbarten der Staatskanzlei, deren Teil die Onlineredaktion des Landesportals in Wirklichkeit ist, ihre höchstpersönlichen Anliegen, die eigentlich gar nicht für diese bestimmt waren. Damit kam es fortwährend zu Datenübermittlungen an eine unzuständige Stelle. Der Landesbeauftragte hatte der Staatskanzlei eine Reihe von Vorschlägen zur Abhilfe unterbreitet, von denen leider nur ein einziger umgesetzt worden war. Der Hinweistext auf der Seite des Kontaktformulars war so geändert worden, dass dem Nutzer deutlicher zu machen versucht wurde, an wen seine Nachricht tatsächlich gesendet werden wird.

Einer der Vorschläge des Landesbeauftragten, und zwar der naheliegendste, war, die Nachricht direkt an die Behörde zu senden, von deren Internetseiten das Kontaktformular aufgerufen worden war.

Erfreut las der Landesbeauftragte später in der Stellungnahme der Landesregierung zu seinem IX. Tätigkeitsbericht (Nr. 2.5), dass die Staatskanzlei den Redakteuren im Landesportal die Möglichkeit eröffnet habe, auch ressorteigene Kontaktformulare einzustellen, was so auch für den Landesbeauftragten gelte. Das wäre die Lösung gewesen. Nur: Davon war bisher weder dem Landesbeauftragten noch den Fachressorts etwas aufgefallen. Eine Nachfrage im Landesrechenzentrum brachte schließlich Klarheit. Die genannte Aussage in der Stellungnahme der Landesregierung stellte lediglich ein Ziel dar, realisiert sei die Lösung tatsächlich bisher nicht. Damit konfrontiert gab die Staatskanzlei schließlich an, dass sie – auch entgegen ihrer eigenen Aussage in der Stellungnahme der Landesregierung zum IX. Tätigkeitsbericht – an der bisherigen Praxis festhalte und über das gesamte Landesportal ein einheitliches Kontaktformular vorhalte, mit dem eine E-Mail an die Onlineredaktion geschickt werden könne.

Der Landesbeauftragte erkennt an, dass der umsichtige Nutzer durch die Formulierung *„…E-Mail an die Onlineredaktion der Staatskanzlei des Landes Sachsen-Anhalt…“* über den Eingabefeldern des Kontaktformulars erfährt, wem er seine Nachricht sendet. Gleichwohl hatten das im Berichtszeitraum wieder 25 Nutzerinnen und Nutzer nicht beachtet und unwissentlich ihre datenschutzrechtlichen Anliegen nicht direkt dem Landesbeauftragten, sondern zunächst den Mitarbeitern der Staatskanzlei anvertraut. Wie hoch die Zahl der für andere Behörden bestimmten Mitteilungen war, die zunächst in die Staatskanzlei gesandt worden waren, ist dem Landesbeauftragten nicht bekannt, sie dürfte jedoch erheblich sein.

Der Landesbeauftragte sieht jedoch die Möglichkeit, dass eine datenschutzrechtlich korrekte Lösung, nämlich das Senden der Kontaktanfragen direkt an das zuständige Ressort, durch einfache Änderungen im Quellcode der Kontaktformular-Seite im Landesportal realisierbar wäre.
In den Quelltext der Webseite mit dem Kontaktformular müsste ein Datenfeld für den Empfänger der E-Mail eingefügt werden, beispielsweise durch einen Auswahlknopf oder ein DropDown-Menü. In dieser Liste müsste jeder mögliche Empfänger aufgeführt werden, der dann per Klick durch den Nutzer auswählbar wäre. Ein im Quelltext besonders markierter Empfänger wäre voreinstellbar. Je nach zugehörigen Webseiten könnte hier sogar automatisch via PHP der wahrscheinlich richtige Empfänger vorausgewählt werden. Nach der Auswertung der Formulardaten im PHP-Quelltext des Formulars würde der Mitteilungstext als E-Mail verschickt.

Der Landesbeauftragte erwartet jedenfalls eine Änderung des bisherigen Zustandes.

14.9 Urteil des Bundesgerichtshofs zur Haftung von WLAN-Betreibern

In seinem Urteil vom 12. Mai 2010 hat der Bundesgerichtshof entschieden, dass Privatpersonen zwar auf Unterlassung, aber nicht auf Schadenersatz in Anspruch genommen werden können, wenn ihr nicht ausreichend gesicher-

ter WLAN-Anschluss von unberechtigten Dritten für Urheberrechtsverletzungen im Internet genutzt wird (NJW 2010, 2061).

Der Bundesgerichtshof hat angenommen, dass eine Haftung als Täter einer Urheberrechtsverletzung nicht in Betracht kommt, weil der Beklagte den fraglichen Musiktitel im Internet nicht zugänglich gemacht hat. Eine Haftung als Gehilfe bei der Urheberrechtsverletzung hätte Vorsatz vorausgesetzt, an dem es im Streitfall fehlte.

Den privaten Anschlussinhabern obliegt jedoch eine Pflicht zu prüfen, ob ihr WLAN-Anschluss durch angemessene Sicherungsmaßnahmen vor der Gefahr geschützt ist, von unberechtigten Dritten zur Begehung von Urheberrechtsverletzungen missbraucht zu werden. Es kann ihnen allerdings nicht zugemutet werden, ihre Netzwerksicherheit fortlaufend dem neuesten Stand der Technik anzupassen und dafür entsprechende finanzielle Mittel aufzuwenden. Ihre Prüfpflicht bezieht sich daher auf die Einhaltung der im Zeitpunkt der Installation des WLAN-Routers für den privaten Bereich marktüblichen Sicherungen.

Diese Pflicht hatte der Beklagte nach Auffassung des Bundesgerichtshofs verletzt, da er es bei den werkseitigen Standardsicherheitseinstellungen des WLAN-Routers belassen und das Passwort nicht durch ein persönliches, ausreichend langes und sicheres Passwort ersetzt hatte. Der Beklagte haftet deshalb nach den Rechtsgrundsätzen der sog. Störerhaftung (Unterlassung und Erstattung der Abmahnkosten).

Das Urteil des Bundesgerichtshofs schafft vor allem für Betreiber öffentlicher Hotspots, die ohne Anmeldung nutzbar sind, Unsicherheit. Sie werden zwar nicht direkt für Urheberrechtsverletzungen Dritter verantwortlich gemacht, aber Abmahnungen oder Verurteilungen zur Unterlassung können bereits hohe Kosten nach sich ziehen.

Der Landesbeauftragte hat bereits in seinem IX. Tätigkeitsbericht die Risiken beim Einsatz von WLAN insbesondere in Verbindung mit lokalen Netzwerken öffentlicher Stellen dargestellt und Hinweise zur Absicherung solcher drahtlosen Netzwerke gegeben (s. Nrn. 14.12 und 14.13).

15 Hochschulen

15.1 E-Mail-Adressen der Hochschule

Eine Pressemitteilung enthielt den Hinweis, dass an einer Universität ein Server im Rechenzentrum umfangreichen Zugriff auf Studentendaten gewähre. Dazu gehören der vollständige Name, das Freischaltungsdatum des Zugangs, die E-Mail-Adresse an der Universität, der Status (Student, Mitarbeiter, inkl. Institut) sowie Gruppen- bzw. Benutzeridentitätsnummern. In kurzer Zeit könnten alle ca. 17.500 Benutzernamen ausgelesen und abgespeichert werden.

Die Universität teilte hierzu mit, dass sie als moderne Einrichtung mit ihren Studenten elektronisch kommunizieren müsse. Demgemäß werde für jeden Studenten ein E-Mail-Postfach „vorname.nachname@st.----.de“ eingerichtet.

Nachdem sich Studenten im Universitätsrechenzentrum angemeldet, ein Passwort ausgesucht und den Nutzungsbedingungen zugestimmt hätten, wäre die Funktionsfähigkeit der E-Mail-Adresse hergestellt und könne in einem sog. LDAP-Verzeichnis durch andere angemeldete Mitglieder der Universität gesucht werden. Ein Rückschluss auf die Person infolge der „sprechenden“ Adresse sei im Hinblick auf leichte Kommunikation gerade erwünscht. Auch in vielen dienstlichen Adresslisten sei ein derartiges Verfahren üblich.
Die Verwendung der elektronischen Dienste der Universität wäre für vielfältige Aktivitäten notwendig (Zugang zum WLAN, zu den Rechnerlaboren, für das Drucken, für E-Learning-Portale). Auch die Kommunikation von Lehrkräften mit Studenten beispielsweise in Bezug auf die Teilnahme an einem Seminar erfolge über die Hochschul-E-Mail-Adresse.

Die Nutzung dieser „sprechenden“ E-Mail-Adresse erscheint im Hinblick auf das Ziel effizienter Kommunikation im Raum der Hochschule durchaus sinnvoll und damit im Rahmen der Aufgabenerfüllung der Hochschule grundsätzlich erforderlich. Bedenken im Hinblick auf Sammlung und Missbrauch der Daten können durch die Verwendung nicht sprechender Adressen allenfalls bedingt ausgeräumt werden. Zudem wäre es bei der Verwendung nicht sprechender E-Mail-Adressen problematisch, im nötigen Umfang Zugriff auf die E-Mail-Clients zu gewähren, die die Zuordnung kennen.

Der Landesbeauftragte hat der Universität daraufhin mitgeteilt, dass die Sicherstellung und Aufrechterhaltung der Trennung des sog. LDAP-Servers vom Internet von besonderer Bedeutung ist, um die weltweite Recherchierbarkeit auszuschließen. Auch innerhalb des universitätsinternen Netzes sollten die Zugriffe rollenbezogen eingeschränkt werden. Auf der LDAP-Ebene sind Berechtigungen sinnvoll zu vergeben, und die Anzahl der Ergebnisdatensätze ist, insbesondere mit Sicht auf die in der Regel zu hohen Vorgabewerte in den Konfigurationsdateien, zu limitieren. Auf Anwendungsebene sind Komplettabfragen zu verhindern. Denkbar wären die Vergabe von Zugängen, erzwungene Wartezeiten abhängig von der Anfragehäufigkeit und Mindestlängen für Suchtexte in Verbindung mit einer zur Erkennung von Datensammlern geeigneten Protokollierung. Die Notwendigkeit einer anonymen LDAP-Nutzung ist zu überprüfen und ggf. abzustellen.

Im Übrigen dürfte davon auszugehen sein, dass die Hochschulmitglieder bzw. -angehörige dieses effiziente Kommunikationssystem gerne und ohne Bedenken nutzen. So wird auch eigenes Tun (Anmeldung im Universitätsrechenzentrum, Aussuchen eines Passworts, Zustimmung zu den Nutzungsbedingungen) vorausgesetzt. Andererseits kann von der Tragfähigkeit einer Zustimmung als Rechtsgrundlage nur dann ausgegangen werden, wenn wirklich Freiwilligkeit vorliegt. Dies setzt voraus, dass Alternativen bestehen. Demgemäß wurde die Universität gebeten, eine Wahlmöglichkeit vorzusehen, sodass auch nicht sprechende E-Mail-Adressen und Benutzernamen auf Wunsch möglich werden.

15.2 Mensakarte eines Studentenwerkes

Durch eine Pressemitteilung wurde der Landesbeauftragte darauf aufmerksam, dass die Mensakarten eines Studentenwerks mit einem Chip ausgerüs-

tet seien, der nunmehr einfach „geknackt“ werden könne. Damit sei der Missbrauch der gespeicherten Daten möglich.
Der Landesbeauftragte hat dies aufgegriffen. Die erste Stellungnahme des Studentenwerkes verwies darauf, dass dort lediglich die Geldbörsenfunktion (Zahlung von Speisen, Nutzung von Waschmaschinen usw.) genutzt würde. Im Übrigen handele es sich um eine von der Universität herausgegebene Karte.
Die Universität teilte mit, dass auf der als Studentenausweis dienenden Karte der Name, die Matrikelnummer und die Bibliotheksnummer abgelegt seien. Weiter gespeichert seien zwei Kartenseriennummern, ein Gültigkeitsdatum sowie der Status für die Essenpreise. Weitergehende personenbezogene Informationen seien nicht gespeichert.

Der Universität wurde empfohlen, auf das Nachfolgeprodukt mit Verschlüsselung nach dem Stand der Technik umzusteigen. Dabei wurde auf § 6 Abs. 1 DSG-LSA hingewiesen. Danach sind die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Im Rahmen der diesbezüglichen Bewertung könne daher berücksichtigt werden, welcher Datenumfang sich auf der Chipkarte befindet und welcher Zugang zu Referenzdateien erforderlich ist, um eine persönliche Zuordnung zu erreichen (z. B. Matrikelnummerliste). Zudem war zu berücksichtigen, dass das Auslesen der nunmehr unsicheren Chipkarte ein sehr starkes Annähern an die Karte mit einem Lesegerät voraussetzt.
Im Einzelnen wurde dargelegt, dass die Verwendung von Klartextdaten auf der Chipkarte problematisch sei. Zur Identifikation könnte ggf. auf die Seriennummer ausgewichen werden. Gegebenenfalls könnte die Einrichtung von Zugangskontrollsystemen (PIN-Abfragen) erfolgen.

Die Universität hat daraufhin mitgeteilt, dass nunmehr Karten mit fälschungssicheren Chips eingeführt würden. Neue Studenten erhielten die neuen Karten. Alte Karten könnten gegen Gebühr ausgetauscht werden.

15.3 Absolventenbefragung

Eine Hochschule plante eine Absolventenbefragung zum Thema „Studienbedingungen und Berufserfolg“. Design und Software kamen von einem Institut der Universität Kassel, das auch die Auswertung durchführen sollte.
Die Hochschule fragte sich zunächst, ob die Nutzung der im Dezernat Studienangelegenheiten vorhandenen Studentendaten der Absolventen des letzten Jahres für die Durchführung einer Absolventenbefragung in der gewünschten Form verwendet werden können. Sie wies u. a. auf die Frage der Spezialität des § 119 HSG LSA hin.

Zu § 119 HSG LSA ließen sich aber keine näheren Hinweise zu einem eventuell abschließenden Charakter finden. § 119 HSG LSA schließt demnach die Anwendung des DSG-LSA für weitere Fragen der Datennutzung oder Verarbeitung nicht aus. Nach § 3 Abs. 3 DSG-LSA sind spezifische Vorschriften nur vorrangig, „soweit“ ihr Regelungsbereich geht. Dem Gesamtkontext des § 119 HSG LSA ist nicht zu entnehmen, dass mit ihm eine abschließende Regelung gemeint sei. Schon der Wortlaut bezieht sich auf die Verpflichtung der Studierenden zur Datenangabe (Übermittlungspflicht), nicht jedoch die

Erhebungsbefugnis der Hochschule. Auch ist beispielsweise die Exmatrikulation als notwendige Hochschulaufgabe nicht erwähnt, obwohl dort eine Datenverwendung notwendig ist. Schwerpunkt der hochschulgesetzlichen Regelung ist eher das Anliegen, den für notwendig erachteten Datenbestand, insbesondere im Hinblick auf die amtliche Statistik, abzusichern.

Nach § 10 DSG-LSA war daher die Verwendung der Daten zulässig, wenn diese vom ursprünglichen Erhebungszweck umfasst wäre. Soweit das Projekt als anderer Zweck gewertet würde, wäre eine Verwendung wohl unzulässig, da nach Angaben der Hochschule kein Forschungsprojekt vorlag und die anderen Regelungen zu möglichen Zweckänderungen nach § 10 Abs. 2 DSG-LSA nicht einschlägig gewesen wären.

Die Zweckidentität ergibt sich aus dem Erhebungsgrund. Der dürfte mangels besonderer Hochschuldatenregelungen in der Absicherung des gesamten Studienverlaufs einer konkreten Person zu sehen sein. Datennutzungen zur Immatrikulation und Exmatrikulation, zur Bibliotheksbenutzung oder zu Prüfungszwecken gehören sicher dazu. Ob die Absolventenbefragung Monate nach dem Ausscheiden noch dazugehört, war fraglich. Nach § 3 Abs. 2 HSG LSA überprüft die Hochschule ständig Inhalte und Formen von Studium und Lehre hinsichtlich neuer Entwicklungen in der beruflichen Praxis. Nach § 3 Abs. 14 HSG LSA ist zur Qualitätsentwicklung regelmäßig eine Selbstevaluation erforderlich. Die Vorschrift betrifft direkt allerdings nur Mitglieder und Angehörige und setzt eine Ordnung voraus. Nach § 7 Abs. 1 HSG LSA ist die Sicherung der Qualität der Lehre regelmäßig durch anonyme Bewertungen vorzunehmen, was allerdings auch eine Ordnung voraussetzt. Weiter können Ergebnisse einer Absolventenbefragung für die Akkreditierung (qualitative Bewertung durch externe wissenschaftliche Einrichtung) von Studiengängen nach § 9 Abs. 3 Satz 4 HSG LSA Verwendung finden. Die Frage, wie Absolventen in der Rückschau ihr Studium bewerten und welchen Erfolg sie damit in der beruflichen Praxis erzielen, ist für Aufgaben der Qualitätssicherung von nicht unerheblicher Bedeutung. Schon dies spricht deutlich für eine Zweckidentität.

Ergänzend ist die Wertung des § 10 Abs. 3 DSG-LSA zu betrachten, wonach bestimmte mit der Hauptaufgabe im engen Zusammenhang stehende Zwecke (Aufsicht, Kontrolle, Organisationsuntersuchung) vom Gesetzgeber ebenfalls nicht als Zweckänderung angesehen werden. Absolventenbefragungen zur Evaluation der eigenen Tätigkeit dürften zumindest ähnlich zu bewerten sein.
Demgemäß war von einer zweckgebundenen Verwendung der vorhandenen Adressdaten auszugehen. Dies bedingt aber zusätzlich, dass die sonstigen Rahmenbedingungen des Gesamtprojektes (Umsetzung und Verfahren) angemessen waren.

Rechtsgrundlage für die Nutzung der Daten war daher § 10 Abs. 1 Satz 1 DSG-LSA. Rechtsgrundlage für eine eventuelle Übermittlung zur Abfrage bei den Meldebehörden für den Fall, dass die Anfragen als unzustellbar zurückkämen, wäre § 11 Abs. 1 DSG-LSA. Die Aufnahme der Rückmeldungen von Meldebehörden rechtfertigt sich auf Grundlage des § 9 Abs. 1 DSG-LSA.

Weiter wurde erörtert, welche der vorhandenen Daten für die Kontaktierung der Absolventen Verwendung finden dürfen. Gegen die Verwendung von Geschlecht und Titel zur Anrede („Frau Dr. …“) bestanden keine Bedenken.
Ebenfalls akzeptabel erschien die Verwendung des Geburtsdatums für Anfragen an die Meldebehörde. Meldebehörden verfügen in der Regel nur über die Erkenntnis, in welchen Meldeamtsbereich die Betroffenen verzogen sind. Um dort die richtigen Personen zu identifizieren, ist zumeist auch das Geburtsdatum erforderlich. Insoweit bestanden ebenfalls keine Bedenken.
Das Vorhaben, auch die Heimatadresse zu verwenden und die Eltern anzuschreiben, um beispielsweise diejenigen zu erreichen, die im Ausland tätig sind, erschien dagegen bedenklich. Die Einbeziehung Dritter in das Kontaktierungsverfahren war problematisch. Betroffene wünschen gelegentlich infolge der familiären Verhältnisse nicht, dass ihre personenbezogenen Daten an die Eltern gehen. Demgemäß gibt die Hochschule auch keine Studienadressen an Eltern heraus. Auf die Verwendung der Elternadressen wurde daher verzichtet.

Ergänzend wurde darauf hingewiesen, dass weitere datenschutzrechtlich relevante Verfahrensfragen zu berücksichtigen sind.
Das vorgesehene Trekking-Verfahren sollte unter dem Aspekt der Datenvermeidung überdacht werden (viermaliger Kontaktversuch). Die zunächst vorgesehene Trennung von Fragebogen und Adresserfassungsseite nach der Rücksendung an die Hochschule durch diese selbst hätte zu personenbezogenen bzw. -beziehbaren Inhaltsdaten geführt.
Weiter sollte bei der Ausgestaltung des Fragebogens bzw. der beigefügten Informationen sichergestellt werden, dass die Betroffenen es vermeiden, bei der Rücksendung des ausgefüllten Fragebogens Identifizierungsmerkmale (Name, Adresse, Immatrikulationsnummer) zu verwenden. Die Betroffenen sollten über das Gesamtkonzept und das angewendete Verfahren informiert sein (Transparenz). Auch müsse auf die frühestmögliche Löschung personenbezogener Daten in der das Projekt durchführenden Organisationseinheit geachtet werden.

15.4 Transferzentren

Die Koordinierung von Wirtschaft und wissenschaftlicher Weiterbildung von Hochschulabsolventen, das Binden von Hochschulabsolventen an die Region und die Absolventenvermittlung stellen Aufgaben dar, die in den Hochschulen des Landes in sog. Transferzentren wahrgenommen werden sollen. Ein wesentliches Arbeitsinstrument der Mitarbeiter der Absolventenvermittlung ist das Portal „http://www.nachwuchsmarkt.de“, ein Stellen- und Praktikaportal im Internet. Es bietet die Möglichkeiten der Suche nach Stellen- und Praktikaangeboten, das Hinterlegen von Bewerberprofilen, die Möglichkeit der Onlinebewerbung und den Zugriff auf Präsentationen von Unternehmen. Entwickler des Portals ist eine private Firma. Der Landesbeauftragte hat das Projekt mit umfänglicher Beratung begleitet.

Die Transferzentren sollten Einrichtungen der Hochschulverwaltungen sein. Infolge dessen war für die jeweilige Hochschule als datenschutzrechtlich verantwortliche Stelle der Hinweis auf §§ 14 und 14a DSG-LSA geboten. Auch wenn das Portal, wie geplant, auf einem externen Server betrieben wird, ist es für die Geltendmachung der datenschutzrechtlichen Rechte der Betroffe-

nen (z. B. Auskunft, Berichtigung, Löschung) geboten, dem Nutzer einen verantwortlichen Ansprechpartner zu benennen. Die Beteiligung der jeweiligen behördlichen Datenschutzbeauftragten erschien angezeigt. Zudem wurde auf die Notwendigkeit der Erstellung eines Verfahrensverzeichnisses hingewiesen.

Infolge der technischen Ausgestaltung des Portals durch Zugriffsregelungen sollte sichergestellt werden, dass grundsätzlich jeweils nur ein Transferzentrum auf die personenbezogenen Daten der Nutzer zugreifen kann. Aus Sicht der Absolventen wäre dies „ihre“ Hochschule, die sie bei der Registrierung und Dateneingabe auswählen. Sie wäre verantwortliche Stelle gegenüber dem Nutzer und setzt dies wiederum durch vertragliche Vereinbarungen mit dem Betreiber des Servers um.
Eine weitere grundlegende Frage betraf die Rechtsgrundlage der Datenerhebung und Verarbeitung durch die jeweiligen Transferzentren. Hier hätte ggf. auf die Vorschriften der §§ 9 ff. DSG-LSA i. V. m. § 3 Abs. 9 HSG LSA abgestellt werden können. Danach wäre eine Datenerhebung und -verarbeitung möglicherweise zulässig gewesen, wenn und soweit dies zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Hierzu sieht die gesetzliche Aufgabenzuweisung nach § 3 Abs. 9 Satz 3 HSG LSA zwar die Bildung von Transferzentren vor, diese dienen jedoch im Hinblick auf Satz 2 dieser Regelung der Förderung der Verarbeitung und Nutzung der Forschungsergebnisse dieser Hochschule. Das Nachwuchsmarktportal dient jedoch allenfalls mittelbar und nur teilweise der genannten Förderung. Primär war es nach den vorliegenden Nutzungsbedingungen als umfänglich wirkendes Personalvermittlungsportal ausgestaltet. Demgemäß erschien es zumindest fraglich, ob der Gesamtumfang des Vorhabens im Rahmen der Aufgabenerfüllung nach § 3 Abs. 9 HSG LSA als erforderlich hätte angesehen werden können. Dies hätte einer umfänglichen fachlichen Bewertung und Begründung bedurft, die jedoch trotz Hinweis ausblieb.

Die Frage nach der gesetzlichen Grundlage konnte aber letztlich dahinstehen, da die Einwilligung als Rechtsgrundlage gewählt wurde. Demgemäß konnte sich die Beratung auf die Ausgestaltung der Einwilligung gemäß den Anforderungen des § 4 Abs. 2 DSG-LSA beziehen.
Es wurde darauf hingewiesen, dass der Nutzer eine im Wesentlichen zutreffende Vorstellung davon haben muss, in welche Datenverarbeitung er einwilligt. Damit die Einwilligung als Rechtsgrundlage tragfähig ist, muss der Nutzer die Bedeutung und Tragweite seiner Entscheidung überblicken können, insbesondere den Umfang des Zugangs Dritter zu den ihn betreffenden Daten abschätzen können.
In den Beratungen wurde daher stets betont, dass ein hohes Maß an Transparenz für die sachgerechte und datenschutzkonforme Ausgestaltung des Portals bedeutsam ist. Der Betroffene sollte die Funktionsweise des Portals und die Zugriffsberechtigungen zumindest grundsätzlich erfassen können.

Der Aspekt der Transparenz erhielt in dem Projekt besondere Bedeutung, da für das Wirken der Transferzentren Verfahrensweisen vorgesehen waren, mit denen ein unbedarfter Nutzer nicht notwendigerweise hätte rechnen müssen. So wurde zunächst in den Erörterungen darauf verwiesen, dass nach bisherigen Erfahrungen Bewerbungen oftmals nicht an der Qualität der Bewerber, sondern an der Qualität der Bewerbung scheitern. Demgemäß war vorgese-

hen, dass die jeweils zuständigen Transferzentren hinsichtlich der von Nutzern hochgeladenen Bewerbungsunterlagen nicht nur Plausibilitätskontrollen durchführen, sondern auch Formulierungshilfen geben. Hierzu wurde vom Landesbeauftragten auf die Notwendigkeit hingewiesen, bei der Versendung von Bewerbungen an Dritte stets, insbesondere aber bei Veränderungen durch das Transferzentrum, die konkrete individuelle Zustimmung des Betroffenen im Einzelfall einzuholen. Der Entwickler des Portals hatte gegenüber dem Landesbeauftragten in Beratungen erläutert, dass dies elektronisch mit angemessenem Aufwand darstellbar sei. Der Verzicht auf das Schriftformerfordernis der Einwilligung nach § 4 Abs. 2 DSG-LSA war insoweit vertretbar, da wegen der besonderen Umstände des Portalverfahrens und vorheriger Einwilligungen die elektronische Zustimmung angemessen erscheint.

Transparenz war weiterhin insoweit geboten, als beabsichtigt war, einen Grunddatenbestand der Stellengesuche allen Transferzentren sichtbar zu machen. Dies sollte dem Zweck dienen, dass auch die vom Stellensuchenden nicht ausgewählten Transferzentren die Möglichkeit haben, den bei ihnen gemeldeten suchenden Unternehmern Hinweise auf potentielle Ansprechpartner im Bereich anderer Hochschulen zu geben.

Zu letzterem Vorhaben hat der Landesbeauftragte darauf hingewiesen, dass zwar die Einwilligung als Rechtsgrundlage für beabsichtigte Datenverarbeitung in Betracht kommen kann, andererseits zu berücksichtigen sei, dass die Hochschulen als öffentliche Stellen der gesetzlichen Vorgabe der Datensparsamkeit und Datenvermeidung (§ 1 Abs. 2 DSG-LSA) Rechnung zu tragen haben. Demgemäß wurde angeregt, die Übermittlung von Stellengesuchen an andere Transferzentren pseudonym auszugestalten. Es dürfe ausreichen, dass die anderen Transferzentren dem Portal unter Verwendung eines Pseudonyms, wie beispielsweise der Identifikationsnummer des Nutzers, mitteilen, dass in ihrem Zuständigkeitsbereich ein zu dem Stellengesuch passendes Stellenangebot eines Unternehmers vorhanden ist. So kann elektronisch die Möglichkeit der Kontaktaufnahme des Stellensuchenden mit dem Stellenbietenden gewährleistet werden, ohne dass Nutzerdaten offen liegen.

Auch zu weiteren Einzelheiten der Nutzungsbedingungen konnten Hinweise gegeben werden. So war u. a. vorgesehen, dass der Nutzer nach Ablauf der Nutzung der Internetplattform mit dem weiteren Erhalt von Informationen oder Anfragen einverstanden sei, wobei das Einverständnis jederzeit widerrufen werden könne. Der Widerruf im Sinne einer Opt-Out-Lösung ist jedoch qualitativ von dem freiwilligen Einverständnis (Opt-In-Lösung) zu unterscheiden. Zur Gewährleistung der vollständigen Freiwilligkeit und zur Vermeidung bedenklicher Koppelungen wurde angeregt, auch hier ein konkret erklärtes Einverständnis einzuholen.

Weiter wurde die Frage der Speicherdauer und der Löschung der Nutzerdaten erörtert. Auf die Verpflichtung zur Löschung von Daten, die für die Aufgabenerfüllung nicht mehr erforderlich sind, wurde hingewiesen.

Darüber hinaus wurde angeregt, die Nutzer durch die Nutzungsbedingungen in die Pflicht zu nehmen. So könnte beispielsweise vorgegeben werden, dass sich der Nutzer mit der Registrierung verpflichtet, die veröffentlichten Daten

oder die übermittelten individuellen Bewerbungen nur für das konkrete Stellenbesetzungsverfahren zu nutzen und danach zu löschen.

Im Übrigen wurden in weiteren Gesprächen mit den Projektverantwortlichen und dem Entwickler detaillierte Aspekte der technisch-organisatorischen Datensicherheit des Portalprojektes erörtert.

16 Kommunalverwaltung

16.1 Datenübermittlung bei der Nutzung von Ratsinformationssystemen

Bereits im VII. Tätigkeitsbericht (Nr. 14.1) informierte der Landesbeauftragte ausführlich über die Grundanforderungen, die Ratsinformationssysteme erfüllen müssen, um einer datenschutzrechtlichen Prüfung stand zu halten.

In der Berichtszeit führte der Landesbeauftragte verstärkt Prüfungen im kommunalen Bereich durch, wobei ein Augenmerk auf die Nutzung dieser Ratsinformationssysteme gelegt wurde.

Fast jede Kommune arbeitet inzwischen mit solchen Systemen, welche von verschiedenen Anbietern zur Verfügung gestellt werden. Stets werden mit den Systemen personenbezogene Daten verarbeitet. So werden die persönlichen Daten der Gemeinde- bzw. Stadtratsmitglieder gespeichert, die Sitzungsunterlagen werden mit diesen Systemen vorbereitet, die Protokolle der Sitzungen damit erstellt, das System wird für die Abrechnung von Sitzungsgeldern für die Gemeinde- und Stadträte genutzt. In den meisten Fällen werden die Sitzungsunterlagen den Gemeinde- und Stadträten zusätzlich zur Möglichkeit des Abrufs über das Internet auch in Papierform zur Verfügung gestellt.

So verschieden hier die Ebenen der Verarbeitung personenbezogener Daten sind, so verschieden sind auch die aufgetretenen datenschutzrechtlichen Probleme.

Es gab Kommunen, die seit Einführung des Systems die Daten ihrer Gemeinde- bzw. Stadtratsmitglieder speichern. Hierzu ist darauf zu verweisen, dass eine Datenspeicherung nach § 10 Abs. 1 DSG-LSA nur zulässig ist, wenn sie „zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind“. Somit sind die Daten, welche für die Erfüllung der Aufgaben nicht mehr benötigt werden, zu löschen (§ 16 Abs. 2 DSG-LSA). Die Daten der aus dem Gemeinde- bzw. Stadtrat ausgeschiedenen Mitglieder dürfen somit nicht bis in alle Ewigkeit in den Systemen gespeichert bleiben, zumal ihre Aktualität – z. B. der Anschrift – nicht gewährleistet ist.

Ein weiteres beobachtetes Problem stellen die Einsichtsrechte in die Sitzungsunterlagen innerhalb der Gemeinde- bzw. Stadtvertretung dar. Zu diesem Thema hat sich der Landesbeauftragte bereits im VIII. Tätigkeitsbericht (Nr. 14.1) geäußert. Werden in den Sitzungsunterlagen personenbezogene Daten erwähnt, müssen auch für die Nutzung der personenbezogenen Daten die Voraussetzungen des § 10 DSG-LSA erfüllt werden.

Ein dritter Schwerpunkt, der bei den Kontrollen aufgefallen ist, ist die Veröffentlichung im Internet. Diese Möglichkeit der Einstellung von Sitzungsunterlagen der öffentlichen Sitzungen und der jeweiligen Protokolle in das Internet stellt ein großes datenschutzrechtliches Problem dar, das scheinbar nicht jedem Bürgermeister bewusst ist.

In den Dokumenten sind nicht nur Namen der Gemeinde- und Stadträte enthalten, sondern auch die der Sachbearbeiter der Gemeinde. In einzelnen Fällen werden auch die Protokolle der Einwohnerfragestunden veröffentlicht.

Es ist fraglich, ob jedem Mitarbeiter und jedem Gemeinde- bzw. Stadtrat bewusst ist, dass seine Meinungsäußerungen über Jahre abrufbar im Internet veröffentlicht werden. Noch fraglicher aber ist, ob ein Bürger davon ausgeht, dass sein Name im Zusammenhang mit seiner Anfrage im Internet veröffentlicht wird. Auch wenn er sich in einer öffentlichen Sitzung äußert, kann nicht davon ausgegangen werden, dass er mit der Veröffentlichung im Internet einverstanden ist. Zumal hier die Öffentlichkeit nicht mehr regional begrenzt ist, sondern ein weltweiter und zeitlich nicht begrenzter Abruf möglich ist.

Gemäß § 56 Abs. 3 GO LSA ist den Einwohnern eine Einsichtnahme in die Niederschriften von öffentlichen Sitzungen zu gestatten. Die Befugnis zur Einsichtnahme ist also auf die Einwohner der Stadt beschränkt, eine Befugnis zur weltweiten Veröffentlichung im Internet lässt sich nicht erkennen.

Findet eine solche Veröffentlichung personenbezogener Daten – die in den Niederschriften, Vorlagen und Beschlüssen enthalten sind – statt, handelt es sich um eine Datenübermittlung an nicht-öffentliche Stellen gem. § 12 DSG-LSA und eine Datenübermittlung ins Ausland gem. § 13 DSG-LSA, da auf das Ratsinformationssystem weltweit von einem unbestimmten Personenkreis zugegriffen werden kann. In der Regel liegen die Voraussetzungen der §§ 12 und 13 DSG-LSA jedoch nicht vor, sodass eine Veröffentlichung personenbezogener Daten im Internet nur zulässig ist, wenn der Betroffene eine Einwilligung nach § 4 DSG-LSA erteilt hat. Liegt keine Einwilligung vor, sind vor der Veröffentlichung der Niederschriften, Vorlagen und Beschlüsse im Internet die entsprechenden personenbezogenen Daten zu entfernen. Im Übrigen gilt der Grundsatz der Datenvermeidung und der Datensparsamkeit gem. § 1 Abs. 2 DSG-LSA, sodass schon bei der Erstellung der Niederschrift geprüft werden sollte, welche personenbezogenen Daten gem. § 56 Abs. 1 GO LSA zwingend enthalten sein müssen und auf welche Daten verzichtet werden kann. So kann z. B. bei einer Frage oder Beschwerde eines Einwohners zu Anliegerpflichten und -rechten die Formulierung „Beschwerde eines Anwohners der …-Straße“ oder auch nur „Frage eines Einwohners“ verwendet werden. Die Prüfung der Berechtigung, an der Einwohnerfragestunde teilzunehmen, kann unabhängig davon erfolgen.

Werden Unterschriftenlisten in die Beratung der Stadt eingebracht, kann im Internet auf die Möglichkeit der Einsicht in die Anlage zur Niederschrift bei der Stadt hingewiesen werden.

Der Landesbeauftragte wird auch in Zukunft bei Kontroll- und Beratungsterminen in den Kommunen die Einhaltung der datenschutzrechtlichen Vor-

schriften bei der Nutzung von Ratsinformationssystemen in den Blick nehmen.

16.2 Übertragung von Gemeinderatssitzungen im Internet

Im Berichtszeitraum wurde unter den Datenschutzbeauftragten die Frage nach der Zulässigkeit der Übertragung öffentlicher Gemeinderatssitzungen im Internet diskutiert.

In der Praxis ist dabei festzustellen, dass der Deutsche Bundestag und verschiedene Landesparlamente wie auch der Landtag Sachsen-Anhalts bereits öffentliche Sitzungen im Internet übertragen. Dagegen ist nichts einzuwenden.

Bei einer Gemeinderatssitzung sind jedoch der begrenzte örtliche Wirkungskreis der Gemeinde und die weltweite Verbreitung der Sitzung im Internet zu bedenken. Sitzungen der Gemeindevertretungen sind nach § 50 GO LSA grundsätzlich öffentlich, jedoch bedeutet Öffentlichkeit in diesem Zusammenhang, dass jeder ohne Rücksicht auf seine Gesinnung oder seine Zugehörigkeit zu einer bestimmten Bevölkerungsgruppe die Möglichkeit hat, an der Sitzung als Zuhörer und Zuschauer teilzunehmen.

Im Ergebnis vertritt der Landesbeauftragte die Auffassung, dass eine Übertragung der öffentlichen Sitzung nur erfolgen darf, wenn alle Beteiligten der Übertragung zugestimmt haben.

In der Entscheidung des Bundesverwaltungsgerichts vom 3. August 1990 (NJW 1991, 118) zur Untersagung der Tonbandaufzeichnung durch einen Journalisten bei öffentlichen Gemeinderatssitzungen wurde hervorgehoben, dass ein öffentliches Interesse daran besteht, „dass die Willensbildung des Rates als demokratisch legitimierter Gemeindevertretung ungezwungen, freimütig und in aller Offenheit verläuft“. Die Befürchtung bestünde, dass „insbesondere in kleineren und ländlicheren Gemeinden weniger redegewandte Ratsmitglieder durch das Bewusstsein des Tonmitschnitts ihre Spontanität verlieren, ihre Meinung nicht mehr „geradeheraus“ vertreten oder schweigen, wo sie sonst gesprochen hätten“. Diese Grundsätze gelten erst recht bei Ton- und Bildaufnahmen, wie es bei einer Übertragung im Internet der Fall ist.

Auch wenn zwischenzeitlich Entscheidungen des Verwaltungsgerichts Saarland, zuletzt vom 25. März 2011 (Az: 3 K 501/10), die Zulassung von Filmaufnahmen bei öffentlichen Stadtratssitzungen zu Sendezwecken durch einen (privaten) regionalen Rundfunkveranstalter für zulässig halten, besteht noch keine rechtliche Grundlage für die Übertragung im Internet.

Bei einer Übertragung der Sitzung im Internet handelt es sich um eine Datenübermittlung ins Ausland, welche in Sachsen-Anhalt in § 13 Abs. 2 DSG-LSA geregelt ist. Da die anderen Voraussetzungen für die Zulässigkeit der Übertragung in der Regel nicht erfüllt sein dürften, bleibt hier nur die Einwilligung aller Betroffenen nach § 13 Abs. 2 Nr. 1 DSG-LSA. Weiterhin sollte bei allen Überlegungen auch die unbefristete Speicherung der übertragenen Gemeinderatssitzung im Internet Beachtung finden.

Es ist also bei einer Übertragung der Gemeinderatssitzung im Internet stets darauf zu achten, dass nur die Gemeinderäte zu sehen und zu hören sind, welche ihre Einwilligung erklärt haben und außerdem Zwischenrufe oder Wortmeldungen z. B. bei einer Einwohnerfragestunde von Einwohnern der Stadt, welche nicht Gemeinderäte sind, von der Übertragung ausgeschlossen sind.

Sollten Gemeinden des Landes Sachsen-Anhalt ein solches Vorhaben in die Praxis umsetzen, wird sich der Landesbeauftragte dies bei seinen Beratungs- und Kontrollterminen ansehen und datenschutzrechtlich bewerten.

16.3 Kontrollkompetenzen des Gemeinderates trotz Datenschutz

Im Rahmen einer Petenteneingabe wurde der Landesbeauftragte um Stellungnahme gebeten, wie das Verhältnis von Kontrollrechten des Gemeinderates zum Datenschutz zu bewerten sei.

Im vorliegenden Fall meinte der Petent, welcher Stadtrat einer Stadt ist, er könne seiner Prüf- und Kontrollpflicht, insbesondere zur Abgabe einer Stellungnahme zum Ergebnis einer überörtlichen Prüfung nach § 44 Abs. 3 Nr. 5 GO LSA nicht nachkommen, da im Prüfbericht vorkommende Namen und Adressen von Einwohnern der Stadt geschwärzt wurden.

Der Landesbeauftragte ließ sich für seine Überprüfung den Prüfbericht in ungeschwärzter sowie in geschwärzter Fassung vorlegen und bat den Bürgermeister und das zuständige Rechnungs- und Gemeindeprüfungsamt um Stellungnahme, auf welcher Grundlage die Schwärzungen vorgenommen wurden.

Nach Auswertung der jeweiligen Stellungnahmen konnte festgestellt werden, dass die vorgenommenen Schwärzungen unter datenschutzrechtlichen Gesichtspunkten nicht unzulässig waren. Das nach § 126 Abs. 1 und 3 GO LSA für den Inhalt und die Form des Prüfberichts verantwortliche Rechnungs- und Gemeindeprüfungsamt des Landkreises hat die Übergabe eines anonymisierten Prüfberichts offensichtlich für ausreichend gehalten, damit der Gemeinderat seinen Prüf- und Kontrollpflichten nach der GO LSA, insbesondere zur Abgabe einer Stellungnahme zum Ergebnis der überörtlichen Prüfung nach § 44 Abs. 3 Nr. 5 i. V. m. § 126 Abs. 5 GO LSA, nachkommen konnte.

Der Landesbeauftragte stellte fest, dass hiermit dem in § 1 Abs. 1 DSG-LSA genannten Ziel, den Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts zu schützen, in besonders auffälliger Weise Rechnung getragen wurde. Da jedoch nicht festgestellt werden konnte, dass dies zum Zweck der Beschneidung der Kontrollkompetenzen des Gemeinderates geschehen ist und laut Mitteilung der Kommunalaufsicht des zuständigen Landkreises auch in der Praxis nicht unüblich ist, konnte keine Verletzung datenschutzrechtlicher Vorschriften festgestellt werden. Im Übrigen liegt der Schwerpunkt der Bewertung im kommunalrechtlichen Bereich.

Allgemein weist der Landesbeauftragte darauf hin, dass die GO LSA verschiedene Möglichkeiten kennt, um die Auskunfts- und Kontrollrechte der Gemeinderäte datenschutzkonform zu gewährleisten. Werden in einem Prüf-

bericht Unregelmäßigkeiten festgestellt, kann die Preisgabe personenbezogener Daten im Einzelfall erforderlich sein, um den Vorgang aufzuklären. Hier kann der Datenschutz durch entsprechende Schutzvorkehrungen, z. B. durch die Beschränkung der Einsicht auf die zur Kontrolle erforderlichen personenbezogenen Daten sowie die Behandlung des Berichts in nichtöffentlicher Sitzung und die damit einhergehende Pflicht eines Gemeinderats zur Verschwiegenheit nach der GO LSA, gewährleistet werden. Ferner ist auf die Informationsrechte der Gemeinderäte (Anfragen und Akteneinsicht) sowie die Unterrichtungspflicht des Bürgermeisters zu verweisen.

17 Landtag

17.1 Prüfung des Landesrechnungshofs zu Aufwandsentschädigungen der Abgeordneten

Aufgrund von zahlreichen Eingaben und Anfragen recherchierte der Landesbeauftragte zu Prüfungen des Landesrechungshofs im Jahre 2010 in der Landtagsverwaltung. Die Prüfung des Landesrechnungshofs bezog sich auf den Ersatz von Aufwendungen an Abgeordnete für die Beschäftigung von Mitarbeiterinnen und Mitarbeitern gem. § 8 Abs. 2 AbgG LSA. Es war der Verdacht formuliert worden, der Landesrechnungshof habe sich in unberechtigter Weise Zugang zu arbeitsvertraglichen Unterlagen verschafft.
Der Präsident des Landesrechnungshofes hatte die Prüfung dem Präsidenten des Landtags schriftlich angekündigt. Dieses Schreiben, das noch keine näheren Details zu den einzusehenden Unterlagen enthielt, hatte der Präsident des Landtags an die Fraktionsvorsitzenden weitergeleitet. Im Folgenden hat der Landesrechnungshof die Einsicht in zahlungsbegründende Unterlagen erbeten. Dem Landesrechnungshof wurde daraufhin von der Landtagsverwaltung die Möglichkeit eingeräumt, in einzelne zur Aufwandsentschädigung für die Beschäftigung von Mitarbeitern geführte Akten Einsicht zu nehmen und Kopien anzufertigen. Dies betraf die Vorgänge mit den Anträgen, den Arbeitsverträgen und den Personalbögen. Andere Vorgänge, beispielsweise mit sozialversicherungsrechtlichem Bezug und Gesundheitsdaten, lagen dem Landesrechnungshof nicht vor.

Rechtsgrundlage für die Datenübermittlung an den Landesrechnungshof war § 95 Abs. 1 LHO. Danach ist die Landtagsverwaltung verpflichtet, dem Landesrechnungshof die Unterlagen vorzulegen, die der Landesrechnungshof zur Erfüllung seiner Prüfungsaufgaben für erforderlich hält. Aufgrund der in Artikel 98 Abs. 1 der Landesverfassung garantierten Unabhängigkeit obliegt die Ausgestaltung der Prüfung grundsätzlich dem Landesrechnungshof. Anhaltspunkte für eine Verletzung der auch vom Landesrechnungshof zu beachtenden verfassungsrechtlichen Grenzen waren nicht gegeben.

Die Erforderlichkeit richtet sich nach der Aufgabenstellung. Nach § 90 LHO obliegt dem Landesrechnungshof die Prüfung der Haushalts- und Wirtschaftsführung, insbesondere der Frage, ob die Ausgaben begründet und belegt sind. Die Einsichtnahme in die vorgelegten zahlungsrelevanten Unterlagen, wie insbesondere Arbeitsverträge, begegnete daher keinen datenschutzrechtlichen Bedenken.

Auch der besondere Status der Abgeordneten als Vertragspartner der Arbeitsverträge stand einer Überprüfung materiell-rechtlich nicht entgegen.
Der Anspruch auf Ersatz tatsächlich entstandener Aufwendungen basiert zwar auf dem Abgeordnetenstatus. Er unterscheidet sich jedoch von der grundlegenden Alimentation der Abgeordneten zur Sicherung der unabhängigen Mandatsausübung. Über Aufwendungsersatzanspruch entscheidet die Landtagsverwaltung als Verwaltungsbehörde auf Antrag und Nachweis.
Auf der Grundlage des § 91 Abs. 1 Nr. 1 LHO ist eine Überprüfung des Landesrechnungshofes auch gegenüber Dritten als Empfänger von Aufwendungsersatz grundsätzlich möglich. Ziel dieser Prüfung ist nicht die Ausforschung des einzelnen Abgeordneten als Empfänger von Aufwendungsersatzleistungen oder gar von deren Mitarbeitern. Nach dem Wortlaut der LHO dient die Erhebung – „bei“ den Stellen, nicht „der“ Stellen – als Erkenntnismittel für die Prüfung der Landtagsverwaltung.

Jedoch hat der Landesbeauftragte angemerkt, dass eine höhere Transparenz hilfreich gewesen wäre, um Missverständnisse zu vermeiden. Die Transparenz gehört zu den grundlegenden allgemeinen Anforderungen des Datenschutzes. Trotz der grundsätzlich erfolgten Informationen wäre es sinnvoll gewesen, eine umfänglichere Aufklärung dahingehend vorzunehmen, dass der Haushaltsvollzug der Landtagsverwaltung, nicht die Abgeordneten und ihre Beschäftigten, geprüft werden.

Infolge von Presseberichten über Internetrecherchen des Landesrechnungshofs zur Verwendung der Entschädigung durch die Abgeordneten nahm der Landesbeauftragte die Prüfung im Sommer 2011 wieder auf.

18 Personalwesen

18.1 Gesetz zur Neuordnung des Landesbeamtenrechts

Im IX. Tätigkeitsbericht (Nr. 17.1) hatte der Landesbeauftragte seine Beteiligung bei der Erstellung des Gesetzentwurfs dargestellt. Die Anregungen wurden überwiegend aufgegriffen. Nunmehr ist das Landesbeamtengesetz seit dem 1. Februar 2010 in Kraft (GVBl. LSA S. 648). Im Hinblick auf das differenzierte Personalaktenrecht ist die Rechtslage weitestgehend gleich geblieben. Ergänzt wurde u. a., dass die Vorlage der Personalakte bei Fällen der Mitwirkung an einer Personalentscheidung nicht nur an Behörden desselben, sondern nun auch eines anderen Dienstherrn möglich ist (§ 88 Abs. 1 Satz 2 LBG LSA). Die Tilgung von Unterlagen über nachteilige Beschwerden, Behauptungen oder Bewertungen erfolgt nunmehr nach zwei Jahren (§ 89 Abs. 1 Nr. 2 LBG LSA).

18.2 Personalmanagementsystem

Der Landesbeauftragte hatte bereits im IX. Tätigkeitsbericht (Nr. 17.2) ausführlich zu den mit dem neuen landesweiten Personalmanagementsystem (genannt PROMIS) verbundenen datenschutzrechtlichen Aspekten Stellung genommen. Er hat den Prozess weiter begleitet, war in den Projektlenkungsgruppensitzungen vertreten und hatte Gelegenheit, mit der Projektleitung direkt datenschutzrelevante Fragen zu erörtern.

Im Rahmen der Erörterungen wurde u. a. festgestellt, dass das einzurichtende Datawarehouse im Hinblick auf das Ziel statistischer Führungsinformationen von vornherein lediglich aggregierte Daten enthalten wird.
Weiterhin wurde mitgeteilt, dass für die aus dem Bezügesystem KIDICAP zu transferierenden Daten sichergestellt werde, dass die Datensätze den jeweiligen ursprünglichen Dienststellen zugeordnet bleiben. Ein behördenübergreifender unberechtigter Zugriff sei damit ausgeschlossen. Hierzu habe eine Zuordnung (Mapping) zu den einzelnen in KIDICAP hinterlegten Dienststellen und Unterdienststellen stattgefunden. Die Darstellung, wie dies technisch sichergestellt wird, steht noch aus.

Die Zugriffe auf personenbezogene Daten werden durch Rollen- und Berechtigungsvergaben strukturiert. Im jeweiligen Ressort soll dezentral festgelegt werden, welcher Person konkret welche Rollen zugeteilt werden. Dies übernehme die jeweilige Kopfstelle des Ressorts. Demgemäß werden die Einhaltung der Vorgaben der §§ 84 Abs. 4, 88 Abs. 1 LBG LSA sowie die Beachtung des Grundsatzes der Datensparsamkeit und des Gebots der informationellen Gewaltenteilung einer dezentralen Betrachtung bedürfen.
Ein Gesamtkonzept zu Berechtigungen und Datenschutz liegt dem Landesbeauftragten vor und dient als Grundlage weiterer Erörterungen. Hier dürften u. a. Aufbewahrungen und Löschungen im Vordergrund stehen. Eine besondere Problematik 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 Transfer 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 geboten.

18.3 Erweiterte Zentralregisterauskunft für Polizeibewerberauswahlverfahren

Im IX. Tätigkeitsbericht (Nr. 17.8) hatte der Landesbeauftragte datenschutzrechtliche Bedenken gegenüber dem Polizeibewerberauswahlverfahren formuliert. Die Bewerber wurden mit einer Belehrung und Einverständniserklärung im Hinblick auf die Hinzuziehung unbeschränkter Auskünfte aus dem Bundeszentralregister konfrontiert. Erfreulicherweise hatte das Ministerium des Innern die Verwendung derartiger Unterlagen umgehend auf die Fälle beschränkt, in denen eine unbeschränkte Auskunft aus dem Bundeszentralregister zur Ablehnung führen sollte.
Weiter hatte der Landesbeauftragte darauf hingewiesen, dass die Einbeziehung einer unbeschränkten Auskunft nach § 41 BZRG in das Bewerberauswahlverfahren als Umgehung der Vorschriften des BZRG anzusehen sein dürfte. Auch die Verwendung sei begrenzt (§ 43 BZRG).

Hierzu hatte die Landesregierung in ihrer Stellungnahme zu Nr. 17.8 des IX. Tätigkeitsberichts mitgeteilt, dass eine Umgehung nicht zu erkennen sei. Lediglich das Ministerium erhalte die Auskünfte zu den Bewerbern, die das bisherige Auswahlverfahren bei der Fachhochschule der Polizei positiv durchlaufen haben. Die Fachhochschule dagegen erhalte lediglich eine Liste der für eine Ernennung in Frage kommenden Bewerber. Gegebenenfalls

könne im Rechtsstreit mit Einwilligung des Betroffenen auf die Auskunft zurückgegriffen werden.

Die Frage nach der zulässigen Verwendung von Bewerberdaten bei Einstellungsverfahren ist ein äußerst facettenreiches datenschutzrechtliches Standardthema. Hier prallen zumeist durchaus legitime Anliegen der Arbeitgeberseite und gewichtige Persönlichkeitsinteressen der Betroffenen aufeinander. Wo der sachgerechte Ausgleich der beteiligten Interessen liegt, wird oft kontrovers diskutiert. Der erste kurze Gedankenaustausch, der sich in den Darstellungen im IX. Tätigkeitsbericht widerspiegelt, konnte die Bedenken des Landesbeauftragten nicht zerstreuen.

§ 41 BZRG erlaubt nach Abs. 1 Nr. 2 grundsätzlich die erweiterte Beauskunftung von obersten Landesbehörden. Nach Abs. 4 ist ein Zweck anzugeben und die Zweckbindung bestimmt. Eine Verwendung für „jeden beliebigen“ Zweck kann aber nicht zulässig sein. Demgemäß ist beim Handeln des Ministeriums jedenfalls der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zu wahren.

Es ist zunächst festzustellen, dass das Bundeszentralregistergesetz die Zwecke für die Verwendung der erweiterten Auskunft überwiegend abschließend formuliert und auch im Hinblick auf weitere Verwendungen enge Grenzen zieht (Zweckbindung nach § 41 Abs. 4, Weitergabebeschränkung nach § 43). Aus wohl erwogenen Gründen, insbesondere dem Aspekt der Resozialisierung und im Ergebnis auch zum Schutz der personenbezogenen Daten der Betroffenen, hat der Bundesgesetzgeber den Zugang zur Kenntnis über geringwertigere Bestrafungen eingeschränkt. Demgemäß stellt sich die Frage, ob nicht die von den obersten Landesbehörden zu benennenden Zwecke ein ähnlich gewichtiges öffentliches Interesse repräsentieren müssten, wie die im BZRG benannten Gründe, um einen derart gravierenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen zu rechtfertigen.
Damit ist letztlich der Aspekt der Umgehung bundesgesetzlicher Vorgaben durch landesgesetzliche Verfahren zu betrachten. § 41 BZRG setzt inhaltlich einen eng begrenzten abschließenden Rahmen für die Verwendung erweiterter Auskünfte. Es erscheint zwar nachvollziehbar, dass der Bundesgesetzgeber die einzelnen Zwecke der obersten Landesbehörden nicht bundesgesetzlich festlegt. Andererseits hat er deutlich gemacht, aufgrund welcher gewichtiger öffentlicher Interessen eine Einschränkung des einzelnen informationellen Selbstbestimmungsrechts und des Resozialisierungsinteresses vertretbar ist. Allgemeine Bewerbungsverfahren gehören nicht dazu. Auch die Änderung in § 41 Nr. 1 BZRG, die zur Aufnahme der Beauskunftung in Bezug auf Strafvollzugsbeamte führte, macht deutlich, dass der Bundesgesetzgeber die Personalauswahlfälle, in denen er den Zugriff gestatten will, ausdrücklich aufführt. Ein weiteres Beispiel hierfür ist § 30a BZRG, der seit dem 1. Mai 2010 für Einrichtungen der Kinder- und Jugendarbeit für Zwecke der Personalüberprüfung die Einholung eines erweiterten Führungszeugnisses vorsieht. Wenn aber das Bundesrecht die Verwendung erweiterter Zentralregisterauskünfte für einfache Bewerbungsverfahren nicht vorsieht, scheint die ministerielle Beschaffung für die beabsichtigte Weiterleitung als Umgehung des Willens des Bundesgesetzgebers rechtsstaatlich bedenklich.

Die Verhältnismäßigkeit wird auch dadurch in Frage gestellt, dass in anderen Bereichen, auch sensiblen Bereichen im öffentlichen Dienst, ein herkömmliches Führungszeugnis für ein ordnungsgemäßes Bewerberauswahlverfahren als hinreichend angesehen wird.
Zudem ergab sich nach Mitteilung des Ministeriums in den letzten drei Jahren bei etwa 900 Einstellungsverfahren nur in vier Fällen ein positiver Befund aus der Auskunft, was dann jeweils zur Nichteinstellung führte.

Da das BZRG nur Verwendungsregelungen und Übermittlungsbefugnisse für das Register enthält, bedürfen die anfordernden Stellen jeweils einer Erhebungsbefugnis. Hierzu verweist das Ministerium auf die beamtenrechtlichen Grundlagen.
Allerdings ist bei der Prüfung der Erforderlichkeit aus datenschutzrechtlicher Sicht ein strenger Maßstab anzulegen (vgl. Nr. 9.1 VV-DSG-LSA). Der geforderten Unerlässlichkeit stehen hier wieder die vorgenannten Bedenken entgegen (Vorgabe des Bundesgesetzes, Resozialisierung, wenige Fälle, mildere Mittel).

Weitere Bedenken ergeben sich daraus, dass die Erhebung von personenbezogenen Daten über Bewerber nach § 84 Abs. 1 LBG LSA im Rahmen des Erforderlichen zwar grundsätzlich zulässig ist, aber fraglich ist, ob die Erhebung nicht zur Erfüllung der Aufgaben der erhebenden Stelle selbst erforderlich sein muss. Erklärter Zweck nach der Stellungnahme der Landesregierung zum IX. Tätigkeitsbericht ist aber die beabsichtigte Weiterleitung der unbeschränkten Auskünfte über abgelehnte Bewerber an die Fachhochschule der Polizei. Unter Umständen solle die Auskunft dann zum Bestandteil des Bewerbungsverfahrens werden. Einstellungsbehörde ist aber die Fachhochschule der Polizei, die dann auch die Personalakten führt. Personalaktenrechtlich ist aus datenschutzrechtlicher Sicht zwischen der das Einstellungsverfahren durchführenden Behörde und der obersten Dienstbehörde zu unterscheiden. Dies tut letztendlich auch § 84 Abs. 1 LBG LSA, der die verwendeten Fragebögen der vorherigen Genehmigung durch die oberste Dienstbehörde unterwirft. Auch die Regelung des § 88 Abs. 1 LBG LSA differenziert eindeutig zwischen der datenschutzrechtlich verantwortlichen personalverwaltenden Dienststelle und der obersten Dienstbehörde. Hier wird gerade die gesonderte Rechtsgrundlage für den Datenfluss zwischen der zuständigen Behörde und der im Rahmen der Dienstaufsicht weisungsbefugten Behörde geschaffen.

Das Ministerium geht dagegen davon aus, dass es den Teil des Bewerbungsverfahrens, der sich auf die erweiterte Auskunft bezieht, wieder an sich ziehen könne. Aus beamtenrechtlicher, aber insbesondere aus staatsorganisationsrechtlicher Sicht ist noch nicht abschließend geklärt, ob diese Änderung des Aufbaus der öffentlichen Verwaltung gerade und nur für die Auskünfte unbedenklich ist, an die die grundsätzlich zuständige Behörde nicht herankommt.

Die Bedenken des Landesbeauftragten wurden auch nicht dadurch zerstreut, dass die Fachhochschule der Polizei vom Ministerium keine ausführlichen Einzeldaten, sondern lediglich die listenmäßige Mitteilung erhält, ob für die Betroffenen die Einstellungsvoraussetzungen vorliegen oder nicht. Im Hinblick auf das erklärte Verfahren ist für diejenigen, deren Einstellung abge-

lehnt wird, die personenbezogene Auskunft damit verbunden, dass eine gerichtliche Bestrafung im Register geführt wird.

Damit ergeben sich weitere Bedenken aus der beabsichtigten Weiterleitung im Hinblick auf die Vorgabe des § 43 BZRG, wonach die Auskünfte nachgeordneten Behörden nur mitgeteilt werden dürfen, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde. Hierzu geht das Ministerium von einer erheblichen Erschwerung öffentlicher Aufgaben aus. Das erscheint aber im Hinblick auf die genannten Zahlen (vier Fälle), die engen Vorgaben des Bundesgesetzgebers und die vielen anderen bedeutsamen Personalauswahlverfahren ohne erweiterte Auskunft mehr als fraglich. Das hohe Ausnahmeniveau des § 43 BZRG für die Weiterleitung kann nicht als erreicht angesehen werden, wenn dem Bewerbungsverfahren lediglich einige niedrigschwellige Verurteilungen entzogen würden.

Weiter erschien fragwürdig, dass die Verwendung der Auskunft im Rechtsstreit mit einem abgelehnten Bewerber zumindest dann vorgesehen ist, wenn dieser in die Übermittlung an die Fachhochschule der Polizei zuvor eingewilligt hat. Erkläre er sein Einverständnis nicht, sei eben nicht die Fachhochschule der Polizei, sondern das Ministerium Verfahrensgegner.
Da die Fachhochschule der Polizei das Bewerbungsverfahren durchführt und Einstellungsbehörde ist, dürften Ablehnungsentscheidung und Rechtsbehelfsbelehrung daher von der Fachhochschule stammen. Eventuelle negative Voten des Ministeriums wären dann ggf. inzident zu überprüfen. Wie das dann aber geschehen soll, wenn der Betroffene sein Einverständnis verweigert, was ihm nach der Belehrung auch nicht zum Nachteil gereichen darf, erscheint fraglich.
Darüber hinaus wäre auch die Tragfähigkeit eines eventuellen Einverständnisses als Rechtsgrundlage fragwürdig, da der Betroffene unter dem Druck der begehrten Einstellung wohl nicht freiwillig handeln kann.

Das nachvollziehbare Anliegen des Ministeriums, auch weniger gewichtige Verurteilungen vor der Einstellung zur Prüfung zur Kenntnis zu bekommen, und die vielfältigen Fragestellungen begründen weiteren Erörterungsbedarf.

18.4 Eingliederungsmanagement und Personalvertretung

Der Landesbeauftragte hatte sich im IX. Tätigkeitsbericht (Nr. 17.10) zu Fragen des Eingliederungsmanagements und der Beteiligung der Personalvertretung geäußert. Aufgrund von einigen obergerichtlichen Entscheidungen wurde empfohlen, die Beteiligung der Personalvertretung erst nach der Zustimmung des Betroffenen vorzunehmen.

Nunmehr hat sich die Entscheidung des Bundesverwaltungsgerichts vom 23. Juni 2010 (Az.: 6 P 8.09; NZA-RR 2010, S. 554) mit der Problematik befasst. Allerdings bezog sich die Entscheidung nur auf die Frage, ob die Personalvertretung einen Anspruch darauf habe, dass ihr ein Anschreiben an Betroffene und deren Antwort ohne vorherige Zustimmung zur Kenntnis gegeben wird. Einen Anspruch auf die Kenntnis der Antworten habe die Personalvertretung mangels Erforderlichkeit nicht.

Nicht umfasst war die Frage, ob die Dienststelle verpflichtet ist, der Personalvertretung ohne vorherige Zustimmung des jeweils Betroffenen mitzuteilen, welche Beschäftigten innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren. Insoweit war die vorausgehende Entscheidung des Verwaltungsgerichts rechtskräftig geworden. Die Entscheidung nimmt jedoch an, dass die Personalvertretung nur bei Kenntnis von jedem Anschreiben die Aufgabe nach § 84 Abs. 2 Satz 7 SGB IX wahrnehmen könne, die Erfüllung der Arbeitgeberpflichten zu überwachen. Die Vorlagepflicht sei daher nicht von der Darlegung eines besonderen Anlasses abhängig, nur so könne etwaigen Verstößen der Dienststelle im Vorfeld effektiv begegnet werden.

Der Landesbeauftragte wurde dazu informiert, dass die Entscheidung im Kreise der Personalreferenten der obersten Landesbehörden erörtert und ggf. entsprechende Übermittlungen empfohlen werden sollten. Es sprach sicher einiges dafür, von einem Anspruch der Personalvertretung auszugehen, zu erfahren, welcher der Beschäftigten die Voraussetzungen des § 84 Abs. 2 Satz 1 SGB IX erfüllt und das an ihn gerichtete Informationsschreiben zur Kenntnis zu erhalten.

Es scheint jedoch fraglich, ob die Einzelfallentscheidung derart generalisierend interpretiert werden kann. „Mit Blick auf die Umstände des vorliegenden Einzelfalles“, so das Bundesverwaltungsgericht, war die Zuleitung aller Anschreiben der Dienststelle an die betroffenen Beschäftigten erforderlich, um die Erfüllung der Aufgaben des Arbeitgebers durch die Personalvertretung nach § 84 Abs. 2 Satz 7 SGB IX zu überwachen. Dass das Unterrichtungsschreiben an die Betroffenen nur mit Zustimmung der Personalvertretung zur Kenntnis gegeben werden könne, sei „nicht zwingend“ vorgegeben. Sinn und Zweck des Zustimmungserfordernisses schließe die Weiterleitung des Hinweisschreibens an die Betroffenen nicht von vornherein aus. Das Grundrecht des Betroffenen auf informationelle Selbstbestimmung sei nicht schrankenlos gewährt. Ein Eingriff sei „im zu entscheidenden Einzelfall“ durch überwiegende gegenläufige Interessen gerechtfertigt. Einmal sei insoweit das Überwachungsrecht nach § 84 Abs. 2 Satz 7 SGB IX zu beachten, das dazu diene, kranken Beschäftigten den Arbeitsplatz zu erhalten. Zudem könne das Gewicht des Eingriffs „aufgrund besonderer Umstände des zu beurteilenden Sachverhalts“ relativiert sein. Das Bundesverwaltungsgericht war auch an die rechtskräftige Feststellung zwischen den Beteiligten zum Anspruch auf Mitteilung, wer ein Fall des Eingliederungsmanagements ist, gebunden.

Der Landesbeauftragte wies das Ministerium des Innern mit der Bitte um Erörterung im Kreis der Personalreferenten auf Folgendes hin:

Durch die Übermittlung des Informationsschreibens an die Betroffenen werden der Personalvertretung sensible personenbezogene Daten bezüglich der Länge der Erkrankung des Betroffenen übermittelt. Hierbei handelt es sich um Gesundheitsdaten, die europa-, bundes- und landesrechtlich einem besonderen Schutz unterliegen (vgl. § 2 Abs. 1 Satz 2 DSG-LSA). Unbeschadet bestehender rechtlicher Ansprüche ist daher insoweit in besonderem Maße das Gebot der Datensparsamkeit und Datenvermeidung (§ 1 Abs. 2 Satz 1 DSG-LSA) zu berücksichtigen. Demgemäß sollte davon abgesehen werden, alle Informationsschreiben an die Betroffenen vorsorglich an die Personalver-

tretung zu übersenden, unabhängig davon, ob die Personalvertretung zu Kontrollzwecken den Informationsanspruch geltend gemacht hat. Dem Persönlichkeitsrecht des ohnehin in der konkreten Situation am schlimmsten Betroffenen sollte zumindest soweit Rechnung getragen werden, wie die Personalvertretung nicht ausdrücklich auf die Übersendung der Informationsschreiben besteht.

Mit einer vorsorglichen Übermittlung von allen Informationsschreiben würde zudem die Dienststelle der Entscheidung der Personalvertretung vorgreifen, inwieweit sie ihrer Überwachungspflicht nach § 84 Abs. 2 Satz 7 SGB IX nachkommen will. Will sie zu diesem Zweck sämtliche Anschreiben an die Betroffenen zur Kenntnis bekommen, so geht das Interesse aller Beschäftigten an der Überwachung durch die Personalvertretung nach den Umständen des Einzelfalls ggf. dem Persönlichkeitsrecht des Einzelnen vor. Eine derartige Vollüberwachung dürfte jedoch nicht regelmäßig geboten sein. Insbesondere in den Dienststellen, in denen eine vertrauensvolle Zusammenarbeit zwischen Dienststelle und Personalvertretung sachgerecht stattfindet, sind durchaus andere Kontrollmethoden denkbar. So kann beispielweise im Hinblick auf die vom Bundesverwaltungsgericht angesprochene Ausgestaltung des Einladungs- und Informationsschreibens an eine gemeinsame Erstellung eines Musteranschreibens zunächst ohne konkreten Namensbezug gedacht werden. Zudem wären auch Stichprobenkontrollen als herkömmliches Kontrollinstrument häufig ausreichend.

Weiter bat der Landesbeauftragte, bei der Erörterung auch folgendes zu berücksichtigen:
Soweit die Personalvertretung von der Dienststelle die vollständige Übermittlung sämtlicher Anschreiben erbittet, sollte von der Personalvertretung lediglich ein Mitglied bestimmt werden, dem die Schreiben zu Kenntnis gegeben werden. Die Beschränkung von Mitteilungen des Dienststellenleiters an die Personalvertretung auf einzelne Personalratsmitglieder ist ein in der Verwaltungsrechtsprechung anerkanntes Mittel, um dem Schutz besonders sensibler personenbezogener Daten der Beschäftigten Rechnung zu tragen. Demgemäß liegt es nahe, im vorliegenden Fall, in dem es um Gesundheitsdaten geht, darauf zurückzugreifen, wie auch das Bundesverwaltungsgericht in der o. g. Entscheidung vorgegeben hat.

18.5 Irrweg einer Lohndaten-CD

Ein Universitätsklinikum bediente sich für die Umsetzung der Vergütungszahlungen für seine Beschäftigten einer Finanzbehörde. Im Rahmen der Vorgangsbearbeitung wurde, wie wohl regelmäßig, zum Ende des Kalenderjahres auf dem internen Postweg eine CD mit Bezügedaten der Beschäftigten (Name, Anschrift, Geburtsdatum, Bankverbindung, Bruttoeinkommen, Nettozahlung für das Gesamtjahr, einbehaltene Steuern usw.) an das Universitätsklinikum versandt. Nachdem die CD beim Universitätsklinikum nicht innerhalb des gewohnten Zeitrahmens einging, wurde auch der Landesbeauftragte über den Vorgang informiert.

Die Überprüfung ergab letztlich, dass die CD nicht an die Hausanschrift des Geschäftsbereichs Personalwesen des Universitätsklinikums, sondern an die zentrale Adresse gesandt worden ist. Unter dieser Adresse war jedoch eine

weitere Bedienstete gleichen Nachnamens wie die Adressatin der Lohndaten-CD beschäftigt, die zwischenzeitlich an einer Hochschule eines anderen Bundeslandes tätig war. Ihr wurde diese CD zunächst nachgesandt. Erfreulicherweise wurde dort der Irrtum bemerkt und die CD an das Universitätsklinikum zurückgesandt, sodass größerer Schaden vermieden worden ist.
Schaden hätte jedoch entstehen können, da die Datensätze zu ca. 3.500 Personen mit den kompletten Lohndaten nicht verschlüsselt auf der CD abgelegt waren.

Erörterungen mit den Beteiligten haben dazu geführt, dass auf das bisherige Verfahren verzichtet wird. Die Übermittlung der für die Personalverwaltung benötigten Aufgaben sollte nun nicht mehr mittels einer CD, sondern per E-Mail erfolgen. Die Verschlüsselung unter Verwendung einer vom Bundesamt für Sicherheit in der Informationstechnik zur Verfügung gestellten Software wurde vorgesehen.
Darüber hinaus sollten weitere verbindliche Regelungen die Transportsicherheit gewährleisten. Unterstützung für die zu erstellenden Vereinbarungen zwischen den Beteiligten bietet dabei eine Handreichung zur Auslagerung von Aufgaben sowie ein Mustervertrag zu Auftragsverhältnissen nach § 8 DSG-LSA, die auch auf der Homepage des Landesbeauftragten eingestellt sind.
Die Finanzbehörde hat zwischenzeitlich Regelungen zur Übermittlung von Daten in ihre Dienstanweisung Datenschutz aufgenommen. Die angestrebte Vereinbarung zwischen der Finanzbehörde und dem Universitätsklinikum lässt auch nach 17 Monaten noch auf sich warten.

18.6 Einkommensnachweis bei der Beihilfe

Eine Eingabe wies auf die Beilage zur Bezügemitteilung „Information zur neuen Bundesbeihilfeverordnung“ hin. Zur Berechnung der Beihilfe für Angehörige des Beihilfeberechtigten sah die Regelung in § 4 Abs. 1 Satz 4 BBhV vor, den Gesamtbetrag der Einkünfte des berücksichtigungsfähigen Angehörigen durch Vorlage einer Ablichtung des Steuerbescheides nachzuweisen. Nach § 120 LBG LSA erhalten Beamte und Versorgungsempfänger Beihilfen nach den für die Beamten und Versorgungsempfänger des Bundes jeweils geltenden Vorschriften. Daher war davon auszugehen, dass nunmehr uneingeschränkt der Nachweis durch Vorlage der Ablichtung des Steuerbescheides für die Geltendmachung von Beihilfen für berücksichtigungsfähige Angehörige notwendig sein würde.

Bedenken gegen dieses Verfahren bestehen insoweit, als durch die Vorlage des Steuerbescheides gegenüber der für die Beihilfe zuständigen Stelle eine Vielzahl von Daten bekannt werden können, die zwar steuerrechtlich relevant sind, ggf. aber über den Zweck der Feststellung der Berücksichtigungsfähigkeit im Rahmen der Beihilfe hinausgehen. Demgemäß wurde die Frage der Verhältnismäßigkeit mit dem zuständigen Ministerium erörtert.

Nach Mitteilung des Ministeriums fand die Bundesbeihilfeverordnung für den Bund sowie für einige andere Länder aufgrund einer entsprechenden Verweisung bereits Anwendung. Über eine mögliche Änderung, die den Nachweis der Einkommensgrenzen des berücksichtigungsfähigen Angehörigen auch durch andere Einkommensnachweise zulasse, die vom Beweiswert

dem des Steuerbescheides gleichkommen, werde allerdings nachgedacht. Zudem sei zu bedenken, dass die Beihilfe als Leistung aus öffentlichen Haushaltsmitteln einer sorgfältigen Prüfung der Voraussetzungen bedarf. Angehörige des Beihilfeberechtigten bedürfen nur dann der Fürsorge des Dienstherren, wenn sie über kein eigenes Einkommen verfügen und nicht wirtschaftlich selbständig sind. Demgemäß sind entsprechend normierte Einkommensgrenzen zu berücksichtigen. Insoweit biete lediglich die Vorlage des Steuerbescheides ein vollständiges Bild der Einkünfte des berücksichtigungsfähigen Angehörigen. Anderweitige Nachweise sind im Hinblick auf die Nichtberücksichtigung einzelner Einkunftsarten ungeeignet. Veränderungen wären zudem nur mit unverhältnismäßig großem bürokratischen Aufwand zu erfassen.

Diese Auffassung erschien im Ergebnis vor allem deshalb vertretbar, weil das zuständige Ministerium zusagte, die Beihilfestellen zu veranlassen, Unkenntlichmachungen von Einzelangaben zuzulassen, solange die Summe des Gesamtbetrages der Einkünfte des betreffenden Ehegatten erkennbar bleibt.

18.7 E-Mail-Verkehr des Personalrats

Ein Personalratsmitglied aus einer Polizeidirektion wandte sich an den Landesbeauftragten wegen des Zugangs von Dienstvorgesetzten und Vertretern zu Informationen aus der Personalratstätigkeit infolge des Zugriffs auf seine E-Mail-Konten.

Aus datenschutzrechtlicher Sicht bestanden grundsätzlich keine Bedenken, dass Dienstvorgesetzte bzw. Vertreter im Falle der Abwesenheit auf den dienstlichen E-Mail-Verkehr der Beschäftigten zugreifen können. Unbeschadet dessen erscheint es jedoch geboten, den Zugriff auf Informationen aus der Personalratstätigkeit zu vermeiden. Soweit daher E-Mail-Dienste für Personalratsangelegenheiten zur Verfügung gestellt und in Anspruch genommen werden, ist die Sicherung vor dem Zugriff Unbefugter erforderlich. Hierzu hatte das Ministerium bereits empfohlen, von der Möglichkeit der Verschlüsselung Gebrauch zu machen. Um auch die Absender von E-Mails an Personalratsmitglieder nicht erkennbar werden zu lassen, erscheint jedoch insbesondere die vom Ministerium vorgeschlagene gesonderte Einrichtung von E-Mail-Adressen für Personalratsmitglieder vorzugswürdig. Ministerielle Unterstützung wurde angeboten. Der Landesbeauftragte geht daher davon aus, dass es den Personalratsmitgliedern der Polizeidirektion mit Unterstützung der Dienststelle künftig möglich sein wird, die Verschwiegenheit in Personalratsangelegenheiten zu wahren.

18.8 E-Mail-Eingangskontrolle

Den Landesbeauftragten erreichte eine Beschwerde darüber, dass in einer Landesbehörde der gesamte E-Mail-Eingang durch eine Mitarbeiterin kontrolliert und sortiert werde.

Die Behörde teilte diesbezüglich mit, dass dieser Vorgang allen Beschäftigten bekannt wäre. Außerdem wäre es eine Selbstverständlichkeit, das Netz nur für dienstliche Zwecke zu nutzen. Eine gelegentliche Nutzung für private

Belange werde aber stillschweigend geduldet. Durch den zentralen Eingang werde sichergestellt, dass auch im Falle kurzfristiger Erkrankung des Empfängers besonders eilbedürftige E-Mails bearbeitet werden. Dazu finde in der Poststelle keine Inhaltskontrolle statt, lediglich Absender, Empfänger und Betreff werden daraufhin überprüft, ob eine Weiterleitung erforderlich ist.

Für die datenschutzrechtliche Beurteilung der E-Mail-Eingangskontrolle ist zunächst von Bedeutung, ob die private Nutzung der dienstlichen E-Mail-Adresse erlaubt bzw. untersagt ist.

Ist nur die dienstliche Nutzung gestattet, spricht aus datenschutzrechtlicher Sicht nichts gegen eine zentrale Poststelle, die die E-Mails an die jeweiligen Mitarbeiter bzw. deren Vertreter oder Abteilungsleiter weiterleitet. Dies wäre vergleichbar mit der Briefpost, die auch in der Poststelle der Behörde geöffnet und verteilt wird. Eine Ausnahme bildet u. a. der Personalrat, dessen E-Mails direkt zugestellt werden.

Ist die private Nutzung explizit erlaubt, wird die Behörde gegenüber ihren Mitarbeitern zum Telekommunikationsdiensteanbieter und muss unter anderem das Fernmeldegeheimnis gem. § 88 TKG beachten. Dies ist auch der Fall, wenn die private Nutzung nur stillschweigend geduldet wird. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Aus diesem Grund stellt die Überprüfung von Absender, Empfänger und Betreff der E-Mail durch die zentrale Poststelle bei einer privaten E-Mail schon eine Verletzung des Fernmeldegeheimnisses dar.

Um das Fernmeldegeheimnis einschränken zu können, müsste jeder Mitarbeiter schriftlich die Einwilligung erteilen, dass seine eingehenden privaten E-Mails über die zentrale Poststelle an ihn weitergeleitet werden dürfen. Dann stünde immer noch das Fernmeldegeheimnis des Absenders der E-Mail in Frage.

Der Landesbeauftragte hat daher empfohlen, die private Nutzung der dienstlichen E-Mail-Adresse in einer Dienstanweisung zu untersagen.

Eine entsprechende Dienstanweisung wurde daraufhin in Aussicht gestellt. Hierzu ist auf die Musterdienstanweisung des Ministeriums des Innern zu verweisen (s. Nr. 25.4).

18.9 Nachteilige Tatsachenbehauptungen in der Personalakte

Will der Arbeitgeber eines nach dem Tarifvertrag der Länder Beschäftigten Beschwerden oder Behauptungen tatsächlicher Art, die für diesen ungünstig sind oder nachteilig werden können, in die Personalakte aufnehmen, dann muss er diesen vor der Aufnahme anhören. Die Äußerung des Beschäftigten ist zu den Personalakten zu nehmen. Diese Pflichten ergeben sich aus § 3 Abs. 6 Sätze 4 und 5 TV-L. Eine entsprechende Regelung enthält im Übrigen das LBG LSA in § 86 für Beamte.

In einem von dem Landesbeauftragten zu prüfenden Fall hatte ein Ministerium einem Beschäftigten in der Probezeit – wie es von der Rechtsprechung gebilligt ist – ohne Angaben von Gründen gekündigt. Allerdings enthielt die Personalakte u. a. nachteilige Aussagen zur fachlichen Eignung des Beschäftigten, die mit ein Kündigungsgrund gewesen waren. Während der Betroffene hierin nachteilige Tatsachenbehauptungen sah, vor deren Aufnahme er hätte gehört werden müssen, vertrat das Ministerium die Auffassung, dass es sich hierbei um reine Werturteile gehandelt habe, bei denen eine Anhörung entbehrlich sei.

Der Landesbeauftragte hat die Auffassung des Ministeriums nicht für überzeugend gehalten. Unter Tatsachen versteht man äußere oder innere Vorgänge, die der Nachprüfung durch Dritte offen stehen. Die Aussagen zur fachlichen Geeignetheit des Betroffenen beschrieben teils äußere Vorgänge, die sich objektiv durch Dritte nachprüfen ließen. Teils betrafen sie Werturteile mit einem Tatsachenkern. Folglich lagen nachteilige Tatsachenbehauptungen vor. Im Übrigen war auch die Argumentation des Ministeriums widersprüchlich, hatte es in einer hausinternen Verfügung ausdrücklich festgestellt, dass für eine ordnungsgemäße Anhörung des Personalrats zur Kündigung des Beschäftigten pauschale schlagwortartige Darlegungen ebenso wenig ausreichten wie reine Werturteile ohne Mitteilung der für die Bewertung maßgeblichen Tatsachen. Folglich war das Ministerium selbst davon ausgegangen, dem Personalrat die für die Kündigung maßgeblichen nachteiligen Tatsachen mitteilen zu müssen.

Eine unterbliebene Anhörung des Betroffenen stellt nach der Rechtsprechung des Bundesarbeitsgerichts einen beachtlichen Verfahrensfehler und keine sanktionslose Verletzung einer bloßen Ordnungsvorschrift dar, denn die Anhörung hat eine Friedensfunktion, die daraus resultiert, dass sich der Arbeitgeber mit der Gegendarstellung des Beschäftigten auseinandersetzen soll (BAG, NJW 1990, 1933). Fraglich ist allerdings, ob ein dauerhafter Entfernungsanspruch besteht. Nach der Rechtsprechung des Bundesarbeitsgerichts ist das fragliche Schriftstück bis zur ordnungsgemäßen Anhörung aus den Personalakten zu entfernen, es kann dann aber nach entsprechender Würdigung des Vorbringens des Beschäftigten ggf. wieder zu den Personalakten genommen werden (BAG, NJW 1990, 1933/1934). Der Landesbeauftragte hat in diesem Zusammenhang das Ministerium gebeten, angesichts der Gesamtumstände zu prüfen, ob auf eine erneute Aufnahme der Blätter nicht verzichtet werden könne, weil sie für die weitere Beurteilung des Petenten überflüssig geworden seien und es ihn in seiner beruflichen Entwicklungsmöglichkeit fortwirkend beeinträchtigen würde (vgl. BAG, Urteil vom 13. April 1988 – 5 AZR 537/86).

In seiner Stellungnahme hat das Ministerium mitgeteilt, dass es nach wie vor davon ausgehe, dass die Aussagen zur fachlichen Geeignetheit keine nachteiligen Tatsachenbehauptungen enthielten. Gleichwohl habe es sich entschlossen, die fraglichen Unterlagen aus der Personalakte zu entfernen und die bisher unterbliebene Anhörung nachzuholen. Nach der erfolgten Anhörung wurden die Unterlagen allerdings wieder zur Personalakte genommen, da sie die maßgeblichen Gründe für die Kündigung dokumentierten und als Nachweis für die ordnungsgemäße Beteiligung des Personalrats dienten.

19 Polizei

19.1 Datenarchivierung bei der PD Ost – „Dessauer Staatsschutzaffäre“

Der 10. Parlamentarische Untersuchungsausschuss hat auf Beschluss des Landtages vom 13. September 2007 (LT-Drs. 5/25/849 B) Untersuchungen zu verschiedenen Aspekten der Arbeit der Polizei des Landes Sachsen-Anhalt durchgeführt. Seinen ca. 250 Seiten – ohne Anlagen – umfassenden Abschlussbericht (LT-Drs. 5/3088) hat der Untersuchungsausschuss dem Landtag von Sachsen-Anhalt vorgelegt, der die Arbeit des Ausschusses daraufhin für beendet erklärt hat.

Die Untersuchungen des Ausschusses betrafen auch die sogenannte Dessauer Staatsschutzaffäre. In diesem Zusammenhang stand der Vorwurf von drei Staatsschützern der Polizeidirektion Sachsen-Anhalt Ost im Raum, von einem Vorgesetzten um die Reduzierung ihres dienstlichen Engagements gegen rechtsextremistische Aktivitäten gebeten worden zu sein.

Der Landesbeauftragte befasste sich aufgrund einer Eingabe mit einem Teilaspekt dieser „Dessauer Staatsschutzaffäre“. Einer der drei betroffenen Staatsschützer hat sich mit der Bitte an ihn gewandt, eine anscheinend daraufhin erfolgte Archivierung von Datensicherungsbändern auf deren datenschutzrechtliche Zulässigkeit hin zu überprüfen.

Mit sehr viel zeitlichem Aufwand hat der Landesbeauftragte die Vorgänge aus dem Jahr 2007 durch das Führen verschiedener Gespräche, das Sichten diverser Unterlagen und die Einsicht in eines der archivierten Magnetbänder rekonstruiert und in seinem Prüfbericht vom 18. Januar 2011 bewertet. Im Ergebnis musste der Landesbeauftragte Verstöße gegen datenschutzrechtliche Vorschriften feststellen, die im Kern auf eine rechtsirrige Auslegung von Vorschriften des DSG-LSA zurückgehen. Die abschließenden Feststellungen bestätigten auch die Aussagen der vorläufigen Stellungnahme des Landesbeauftragten als Sachverständiger vor dem Untersuchungsausschuss.

Zum Sachverhalt ist zunächst festzuhalten, dass entgegen Darstellungen in der Presse keine gesonderte Sicherung von Daten auf den Servern der Polizeidirektion stattfand. Es wurden allerdings die zur regulären, und datenschutzrechtlich nicht zu beanstandenden, Datensicherung gefertigten Sicherungsbänder (sog. Backup) auf Weisung in einem verschlossenen Panzerschrank über Jahre aufbewahrt, um sie ggf. für die Aufklärung von Fragen im Zusammenhang mit der „Dessauer Staatsschutzaffäre“ zu verwenden. Eine solche Aufbewahrung ist ein Speichern i. S. d. DSG-LSA, zu einer Verwendung der Daten kam es jedoch nie. Auf den Datensicherungsbändern wurden auch keine E-Mail-Verbindungsdaten gesichert. Der separate E-Mail-Server war in die reguläre Datensicherung nicht einbezogen.

Trotzdem bleiben als datenschutzrechtliche Verstöße festzustellen:

1. Der Zweck der Datenarchivierung war von den Vorschriften nicht gedeckt.

   Daten der Datensicherung (Backup) unterliegen nach § 10 Abs. 4

DSG-LSA einem besonderen Schutz. Grundsätzlich dürfen Daten der Datensicherung nicht für andere Zwecke verwandt werden. Ausnahmen sind nur in einem äußerst begrenzten Umfang zulässig. Die Daten der Datensicherung sind noch enger an die Verwendung für ihren Ursprungszweck gebunden, als es schon grundsätzlich bei personenbezogenen Daten der Fall ist.

Die Polizeidirektion ist rechtsirrig davon ausgegangen, dass die Verwendung der Daten für sonstige Aufsichts- und Kontrollbefugnisse keine Änderung des Verwendungszweckes darstellt. Dem ist aus datenschutzrechtlicher Sicht jedoch nicht zu folgen.

2. Die Dauer der Aufbewahrung der Datensicherungsbänder ist rechtswidrig.

   Die Archivierung der Datensicherungsbänder erfolgte im Mai 2007. Die gespeicherten Daten hätten bereits aufgrund der Unzulässigkeit ihrer Speicherung gelöscht werden müssen. Dieser Löschverpflichtung ist die Polizeidirektion jedoch nicht nachgekommen, weil sie eine eventuelle Verwendung der Daten für disziplinarische Ermittlungen im Zusammenhang mit der „Dessauer Staatsschutzaffäre“ nicht ausschließen wollte.

   Für den Zeitraum ab Juni 2010 bis zum Abschluss der Prüfung durch den Landesbeauftragten muss die Aufbewahrung der Daten allerdings als zulässig gelten, weil der Landesbeauftragte sie für seine Prüfung benötigte.

3. Der Umfang der Datenarchivierung ist datenschutzrechtlich nicht zu vertreten.

   Nach den Erkenntnissen des Landesbeauftragten wurden insgesamt Daten von 243 Bediensteten der Polizeidirektion Sachsen-Anhalt Ost am Standort Kühnauer Straße 161 durch die Datenarchivierung erfasst. Die Auffassung der Polizeidirektion, dass den Bediensteten durch die heimliche Archivierung kein Nachteil entstanden sei, ist nicht grundrechtskonform. Jede Erhebung und Verarbeitung personenbezogener Daten ist nach der Rechtsprechung des Bundesverfassungsgerichtes grundrechtsrelevant. Unverhältnismäßig ist insoweit die Streubreite der Datenarchivierung, weil gegen die nicht von der „Dessauer Staatsschutzaffäre“ betroffenen 240 Bediensteten zu keinem Zeitpunkt Verdachtsmomente bestanden.

Der Landesbeauftragte hat die Polizeidirektion Sachsen-Anhalt Ost, das Ministerium des Innern und den 10. Parlamentarischen Untersuchungsausschuss über die Ergebnisse seiner Prüfung unterrichtet. Die Polizeidirektion wurde darüber hinaus aufgefordert, die Datensicherungsbänder zu vernichten und die erfolgte Vernichtung dem Landesbeauftragten zu bestätigen. Mit Schreiben der Polizeidirektion Sachsen-Anhalt Ost vom Februar 2011 hat diese die Vernichtung der Datensicherungsbänder bestätigt und im März 2011 auch darüber informiert, dass die in Bezug auf die Datenarchivierung

vorliegenden Auskunftsersuchen zweier beteiligter Polizeibediensteter nach § 15 DSG-LSA zwischenzeitlich abschließend beschieden wurden.

19.2 Änderung des SOG LSA

Bereits in den zwei vorangegangenen Tätigkeitsberichten (VIII. Tätigkeitsbericht, Nr. 17.1, und IX. Tätigkeitsbericht, Nr. 18.1) hat der Landesbeauftragte ausführlich dargestellt, warum und welchen Änderungsbedarf er bezüglich des SOG LSA sieht.

Unter der Maßgabe, dass bereits im Dezember 2009 die Einleitung eines Kabinettsverfahrens vorgesehen sei, wurde dem Landesbeauftragten Ende November 2009 der Referentenentwurf eines Änderungsgesetzes zum SOG LSA mit der Bitte um kurzfristige Stellungnahme übersandt. Anfang Dezember 2009 hat der Landesbeauftragte seine Stellungnahme dem Ministerium des Innern zugesandt.

Weil dem Landesbeauftragten seit diesem Zeitpunkt keine Mitteilungen über den Fortgang des Verfahrens vorlagen, hat er im April 2010 beim Ministerium des Innern zum Sachstand angefragt. Im Mai 2010 erhielt er von dort die Information, dass entgegen der ursprünglichen Planungen derzeit eine Änderung des SOG LSA nicht als sachdienlich angesehen wird.

Diese Einschätzung teilt der Landesbeauftragte nicht. Wie bereits im IX. Tätigkeitsbericht erläutert, entspricht die bestehende Rechtslage nicht mehr den Anforderungen, die durch die Rechtsprechung aufgezeigt wurden. Letztendlich muss der Landesbeauftragte wiederum feststellen, dass verfassungsgemäß und sachgerecht ausgestaltete Normen zwingend sind und für das SOG LSA dringender Handlungsbedarf vor allem mit Blick auf die Anwender besteht.

Die Koalitionsvereinbarung für die 6. Wahlperiode des Landtages von Sachsen-Anhalt enthält eine lange Aufzählung von zusätzlich gewünschten Eingriffs- und Datenerhebungsbefugnissen der Polizei. Dieser Katalog erscheint dem Landesbeauftragten als zu einseitig; die Beteiligung bei einem konkreten Gesetzesvorhaben bleibt abzuwarten.

19.3 Beschwerdestelle Polizei

Bereits in seinem IX. Tätigkeitsbericht (Nr. 18.8) hat der Landesbeauftragte über den Entwicklungsprozess zur Bildung einer Beschwerdestelle Polizei berichtet. Der Prozess wurde mit dem Errichtungserlass vom 12. August 2009 abgeschlossen.

Die Beschwerdestelle Polizei wurde – auch wenn verschiedene Modelle lange diskutiert wurden – letztendlich als Stabsstelle beim Staatssekretär des Ministeriums des Innern des Landes Sachsen-Anhalt eingerichtet. Sie nahm ihre Arbeit am 1. September 2009 auf. Räumlich ist die Beschwerdestelle Polizei vom Haupthaus des Ministeriums getrennt untergebracht. Die Beschwerdestelle Polizei hat ihren Sitz beim Technischen Polizeiamt. Die Beschwerdestelle Polizei soll in allen Beschwerdefällen, die die Polizei des Landes Sachsen-Anhalt betreffen, Ansprechpartner sein. Und das nicht nur

für Bürger, sondern auch für Polizisten. Gerade vor dem Hintergrund der Funktion als Ansprechpartner für Mitarbeiter der Polizei erscheint die räumliche Abtrennung der Beschwerdestelle Polizei von der Polizeiabteilung des Ministeriums des Innern des Landes Sachsen-Anhalt eine sinnvolle Lösung zur Wahrung auch datenschutzrechtlicher Belange zu sein.

Im April 2010 hat sich der Landesbeauftragte durch einen Besuch dann ein eigenes Bild von der Arbeit der Beschwerdestelle Polizei gemacht. Der Informationsbesuch war darauf gerichtet, zunächst die Arbeitsweise der Beschwerdestelle Polizei kennenzulernen.

Im Ergebnis dieses Besuchs musste der Landesbeauftragte auf verschiedene datenschutzrechtlich bedenkliche Verfahrensweisen hinweisen. In Gänze betrachtet handelte es sich aber um weniger schwerwiegende Bedenken, die der Landesbeauftragte gegenüber der Beschwerdestelle Polizei geltend machen musste. Zudem hat die Beschwerdestelle Polizei zeitnah auf die Bedenken des Landesbeauftragten reagiert und auf ein datenschutzgerechtes Vorgehen umgestellt.

Beispielhaft für die Feststellungen des Landesbeauftragten soll hier angeführt sein, dass die Beschwerdestelle Polizei auf per E-Mail eingereichte Beschwerden auch ausschließlich per E-Mail reagierte. Datenschutzrechtlich ist die Übermittlung personenbezogener Daten über den unsicheren Übermittlungsweg E-Mail grundsätzlich nur zulässig, wenn eine entsprechende Verschlüsselung erfolgt. Da diese aber derzeit durch die Beschwerdestelle Polizei aus technischen Gründen nicht sichergestellt werden kann, wurde das Verfahren geändert. Zwar erhält der Beschwerdeführer, der seine Beschwerde per E-Mail übersendet, seine Eingangsbestätigung noch immer per E-Mail. In dieser E-Mail wird aber jetzt darauf hingewiesen, dass weiterer Schriftverkehr aus datenschutzrechtlichen Gründen auf postalischem Weg erfolgt.

19.4 Gesprächsaufzeichnungen bei der Polizei

Bereits in seinem VIII. Tätigkeitsbericht (Nr. 17.3) machte der Landesbeauftragte auf die teilweise rechtswidrige Aufzeichnung von Gesprächen (Telefongespräche und Sprechfunkverkehr) aufmerksam. Der Landesbeauftragte wies darauf hin, dass das Ministerium des Innern damals in Aussicht gestellt hatte, eine einheitliche Struktur mit landeseinheitlicher Technik, zentralem Management und dezentraler Aufzeichnung einzurichten.

Erwartungsgemäß nahm die Umstellung eines so großen Verwaltungsbereiches, wie es die Polizei des Landes Sachsen-Anhalt darstellt, einige Zeit in Anspruch. Erst musste sich ein Bild von den Erforderlichkeiten vor Ort, dann von den technischen Möglichkeiten gemacht werden. Anschließend musste die Beschaffung entsprechender Technik ausgeschrieben, gekauft und installiert werden. Parallel zu diesen eher praktischen Fragen mussten jedoch auch die Rahmenbedingungen, innerhalb derer die Technik zu nutzen ist, definiert werden.

So wurde am 12. Dezember 2007 der Runderlass des Ministeriums des Innern zur „Aufzeichnung von Anrufen über Notrufeinrichtungen, sonstigen An-

rufen und des Sprechfunkverkehrs bei der Polizei“ (MBl. LSA 2008 S. 40) erlassen. Der letztendlich veröffentlichten Fassung dieses Erlasses ist eine ausführliche Diskussion zwischen dem Landesbeauftragen und dem Ministerium des Innern über einzelne Regelungen vorausgegangen. Insbesondere die Frage nach der Rechtsgrundlage für die Aufzeichnung des Sprechfunkverkehrs der Polizei erwies sich als wiederholt erörterungsbedürftig.

Im Juli 2009, nachdem der ganz überwiegende Teil der Polizeidienststellen mit der neuen Aufzeichnungstechnik ausgerüstet war, hat der Landesbeauftragte eine dieser Polizeidienststellen zu einem Informationsgespräch, verbunden mit einer Kontrolle hinsichtlich der Aufzeichnung von Gesprächen, aufgesucht. Im Ergebnis konnte der Landesbeauftragte feststellen, dass die betroffene Polizeidienststelle im Rahmen der Umsetzung des vorstehend näher bezeichneten Erlasses datenschutzrechtlichen Belangen Rechnung trägt.

Zum neuen Verfahren zur Gesprächsaufzeichnung konnten die nachfolgenden wesentlichen Aussagen getroffen werden:

Alle Aufzeichnungen (Notrufe, Gespräche zur und von der Rettungsleitstelle des Landkreises, sonstige Gespräche, Sprechfunkverkehr) erfolgen zentral auf einem Server beim Technischen Polizeiamt. Datenschutzrechtlich verantwortliche Stelle für das „Digitale Sprachaufzeichnungssystem der Polizei des Landes Sachsen-Anhalt“ ist das Landeskriminalamt.

Aufgezeichnet werden alle eingehenden Notrufe automatisch. Über die Notrufe hinaus werden richtungsunabhängig (eingehend und ausgehend) alle Gespräche, die zwischen der Rettungsleitstelle des Landkreises und der Polizeidienststelle geführt werden, aufgezeichnet.

Für alle sonstigen Gespräche besteht eine manuell zuschaltbare Aufzeichnungsmöglichkeit an nur einem Apparat in der Polizeidienststelle. Kommen Telefonate an, bei denen der Dienstgruppenleiter eine Aufzeichnung für erforderlich hält, kann er die Speicherung des Gespräches durch das Betätigen einer Taste am Apparat veranlassen. Diese Möglichkeit kann z. B. bei Drohanrufen o. ä. von Bedeutung sein.

Der Sprechfunkverkehr der Polizei wird in Gänze aufgezeichnet.

Gesprächsaufzeichnungen können bis zu fünf Stunden nach der Aufzeichnung mit der entsprechenden Kennung und dem zugehörigen Passwort in der Polizeidienststelle selbst abgefragt werden. Diese Zugriffsmöglichkeit dient in erster Linie dem Nachprüfen von Angaben (Name, Straße, Hausnummer, ...), die während des Gesprächs ggf. nicht deutlich zu verstehen waren oder aus sonstigen Gründen nochmals überprüft werden müssen. Für zwei Bedienstete der zuständigen Polizeidirektion besteht darüber hinaus die Möglichkeit, die Aufzeichnungen bis zu 28 Tage rückwirkend abzufragen und ggf. Arbeitskopien anzufertigen. Eine Überprüfung dieser Vorgaben an einem Rechner durch den Landesbeauftragten hat bestätigt, dass mit der Zugriffsberechtigung der Polizeidienststelle lediglich Aufzeichnungen bis zu ca. fünf Stunden rückwirkend und mit der Zugriffsberechtigung der Polizeidirektion 28 Tage rückwirkend abgehört werden konnten. Für Gespräche, die über den jeweiligen Zeitraum hinausgehen, können nur noch die eigentlichen Ge-

sprächsdaten (Datum, Zeitpunkt, Dauer, eingehend oder ausgehend) aufgerufen werden. Ein Abhören des Inhalts ist nicht mehr möglich.

Datenschutzrechtlich bestehen beim Landesbeauftragten gegen das Verfahren derzeit keine Bedenken.

19.5 Ermittlungsgruppe Schulweg – Teil III

In seinem VIII. (Nr. 18.10) und IX. Tätigkeitsbericht (Nr. 18.14) hatte der Landesbeauftragte die Arbeit der Ermittlungsgruppe Schulweg bei der Polizeidirektion Sachsen-Anhalt Süd vorgestellt und datenschutzrechtlich bewertet. Datenschutzrechtlich war das Vorgehen der Ermittlungsgruppe grundsätzlich nicht zu beanstanden. Änderungswünschen des Landesbeauftragten ist die Ermittlungsgruppe nachgekommen.

Nach § 98b der StPO war der Landesbeauftragte nach Beendigung der Rasterfahndung zu unterrichten, weil er für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei der öffentlichen Stelle Polizeidirektion Sachsen-Anhalt Süd zuständig ist. Dieser Verpflichtung ist die Polizeidirektion Sachsen-Anhalt Süd mit Schreiben vom 6. August 2010 nachgekommen.

Nach Abschluss der Ermittlungstätigkeit im Rahmen der Rasterung wurden durch die Polizeidirektion Sachsen-Anhalt Süd die Arbeitsdatei, die Sicherungsdateien und alle temporären Dateien durch mehrfaches Überschreiben sicher gelöscht. Die Datenträger, auf denen die Daten für die Rasterung angeliefert wurden, wurden bis zum 30. Juli 2010 entweder an die Anlieferer zurückgegeben oder physikalisch – durch Zerstörung – vernichtet.

Der Landesbeauftragte sieht die datenschutzrechtliche Begleitung dieser nicht alltäglichen polizeilichen Maßnahme damit als abgeschlossen an.

19.6 Videoüberwachung am Hasselbachplatz in Magdeburg

In seinem IX. Tätigkeitsbericht (Nr. 18.6) hatte der Landesbeauftragte ausführlich dargestellt, dass und warum die Polizei des Landes Sachsen-Anhalt den Hasselbachplatz in Magdeburg mit einer Videoüberwachungsanlage ausgerüstet hat und diesen seit 2008 überwacht. Der Landesbeauftragte hatte darüber hinaus in Aussicht gestellt, sich zu den Erkenntnissen, die eine Videoüberwachung rechtfertigen sollen, berichten zu lassen.

Im Berichtszeitraum wurde die polizeiliche Anordnung zur Videoüberwachung des Hasselbachplatzes jeweils halbjährlich verlängert. Die Begründungen liegen dem Landesbeauftragten vor. Da es sich bei den vorliegenden Unterlagen allerdings um polizeiinterne Verfügungen handelt, soll an dieser Stelle nur auf die zusammenfassende Einschätzung der Polizei abgestellt werden. Danach sei der Abschreckungseffekt noch nicht in dem gewünschten Umfang eingetreten. Daraus begründe sich weiterer verstärkter polizeilicher Handlungsbedarf und die Notwendigkeit der Weiterführung der Maßnahme.

Die vorliegenden Begründungen rechtfertigen die Fortsetzung der Videoüberwachung auch unter Berücksichtigung datenschutzrechtlicher Belange

derzeit noch. Die künftige Entwicklung wird der Landesbeauftragte aber weiter beobachten.

In diesem Zusammenhang verweist der Landesbeauftragte auch auf seinen Beitrag Nr. 19.4 im IX. Tätigkeitsbericht und die instruktiven Entscheidungen des Oberverwaltungsgerichts Münster vom 8. Mai 2009 (16 A 375/07, RDV 2009, 232), des Hamburgischen Oberverwaltungsgerichts vom 22. Juni 2010 (4 Bf 276/07) und des Verwaltungsgerichts Hannover vom 14. Juli 2011 (10 A 5452/10).

19.7 Auskunftsersuchen des Landeskriminalamtes

Im Rahmen des jährlich durchgeführten Erfahrungsaustausches des Landesbeauftragten mit den behördlichen Datenschutzbeauftragten der Landkreise wurde bekannt, dass das Landeskriminalamt ein Auskunftsersuchen an die Ausländerbehörden der Landkreise gerichtet hat. Die Ausländerbehörden wurden damit gebeten, zur Bekämpfung von Straftaten gegen die äußere Sicherheit der Bunderepublik Deutschland eine Übersicht aller Studenten bestimmter Herkunftsländer mit Angaben des Namens, der Anschrift und der Arbeitsstelle bzw. Studieneinrichtung zu übermitteln.

Zur Aufklärung des Sachverhaltes hat sich der Landesbeauftragte an das Ministerium des Innern des Landes Sachsen-Anhalt gewandt. Der dort bekannte Sachverhalt war zum Zeitpunkt der Anfrage des Landesbeauftragten einer rechtlichen Überprüfung bereits unterzogen worden. Im Ergebnis wurde zwischen dem Ministerium und dem Landeskriminalamt vereinbart, künftig von derartigen Auskunftersuchen abzusehen.

Das Ministerium des Innern des Landes Sachsen-Anhalt hat am 1. Februar 2011 das Landesverwaltungsamt – als Aufsichtsbehörde über die Ausländerbehörden der Landkreise – darüber informiert, dass die konkrete Anfrage des Landeskriminalamtes gegenstandslos sei. Das Landeskriminalamt habe von einer Datenerhebung abgesehen, und es seien auch künftig derartige Ersuchen nicht mehr zu erwarten.

Der Landesbeauftragte musste in diesem Fall aus datenschutzrechtlicher Sicht nicht mehr intervenieren. Unabhängig von der polizeifachlichen und ausländerrechtlichen Bewertung des Auskunftsersuchens bestehen auch aus datenschutzrechtlicher Sicht erhebliche Bedenken gegen die vorsorgliche Erfassung aller ausländischen Personen aus bestimmten Herkunftsländern ohne Verdachtsmomente gegen den Einzelnen.

19.8 Löschung von Daten aus vom BKA geführten Verbunddateien

Was sind Verbunddateien? Als Verbunddateien werden solche Dateien bezeichnet, die für den elektronischen Datenverbund der Polizeien des Bundes und der Länder betrieben werden. Bund und Länder nutzen bestimmte polizeiliche Dateien gemeinsam. Das Bundeskriminalamt (BKA) ist die sogenannte Zentralstelle für den elektronischen Datenverbund. Es stellt die erforderlichen technischen Rahmenbedingungen für sich und alle Bundesländer zur Verfügung. Der Bund und jedes Bundesland geben dann im Rahmen der jeweils für sie geltenden Rechtslage Daten in Verbunddateien ein und stellen

sie damit auch den anderen Verbundteilnehmern zum Abruf im Rahmen von deren Aufgabenerfüllung zur Verfügung.

Die datenschutzrechtliche Verantwortung für diese beim BKA gespeicherten Daten obliegt den Stellen, die die Daten unmittelbar eingegeben haben. Jedes Bundesland bleibt somit verantwortlich für die Rechtmäßigkeit der Erhebung der Daten, die Zulässigkeit ihrer Eingabe in die Verbunddatei, die Richtigkeit und die Aktualität der Daten. Die datenschutzrechtliche Verantwortlichkeit erstreckt sich aber nicht nur auf das Einstellen und Aktualisieren der personenbezogenen Daten, sondern auch auf das Löschen. Das Bundesland, welches die Daten eingeben hat, hat auch die Löschung der Daten vorzunehmen, wenn diese nach den landesrechtlichen Vorschriften nicht mehr in der Verbunddatei vorgehalten werden dürfen. Regelmäßig wird das nach Ablauf bestimmter Löschfristen erfolgen, die allerdings immer dann neu zu laufen beginnen, wenn zu den bisherigen Erkenntnissen neue hinzutreten. Die Systematik ist ähnlich der der „Verkehrssünderkartei“ in Flensburg. Wenn man zwei Punkte bekommen hat, können diese nach zwei Jahren wieder gelöscht werden. Wenn aber innerhalb der zwei Jahre ein weiterer Punkt hinzukommt, beginnt dann die Frist für drei Punkte neu.

Streitig war in diesem Zusammenhang über Jahre hinweg, welche Arten von Daten in Verbunddateien gespeichert werden dürfen, weil es an einer entsprechenden Rechtsverordnung nach § 7 Abs. 6 BKAG mangelte. Nach § 7 Abs. 6 BKAG bestimmt das Bundesministerim des Innern mit Zustimmung des Bundesrates durch Rechtsverordnung das Nähere über die Art der Daten, die in Dateien des BKA als Zentralstelle gespeichert werden dürfen. Die Rechtsprechung – zuletzt das Oberverwaltungsgericht Lüneburg in seinem Urteil vom 16. Dezember 2008, 11 LC 229/08 – ging davon aus, dass die Speicherung von Daten in den Verbunddateien unzulässig ist, solange die erforderliche Rechtsverordnung nicht erlassen wurde. Unzulässig gespeicherte Daten sind nach § 32 Abs. 2 BKAG zu löschen. In der Konsequenz wären alle in Verbunddateien beim BKA gespeicherten Daten zu löschen gewesen.

Die Revision gegen das Urteil des Oberverwaltungsgerichtes Lüneburg (im konkreten Fall ging es um die Verbunddatei „Gewalttäter Sport“) vor dem Bundesverwaltungsgericht hatte jedoch Erfolg. Nicht weil das Oberverwaltungsgericht Lüneburg die zum Zeitpunkt seiner Entscheidung bestehende Rechtslage falsch beurteilt hätte, sondern weil das Bundesministerium des Innern im letzten Moment eine entsprechende Rechtsverordnung erlassen hat, welche durch das Bundesverwaltungsgericht zu berücksichtigen war. Das Bundesverwaltungsgericht führte die mündliche Verhandlung zur Revision am 9. Juni 2010 durch. An diesem Tag trat auch die „Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen“ (BKADV) vom 4. Juni 2010 (BGBl. I S. 716) in Kraft. Damit waren die vorgehaltenen Daten nicht mehr als dem Grunde nach unzulässig gespeichert anzusehen und die Revision – Bundesverwaltungsgericht, Urteil vom 9. Juni 2010 (6 C5/09, NJW 2011, 405) – hatte Erfolg.

Mit dem Erlass der BKADV ist die Bundesregierung auch einer Forderung der Datenschutzbeauftragten des Bundes und der Länder nachgekommen, die diese zuletzt mit ihrer Entschließung „Die polizeiliche Datenverarbeitung

in INPOL hat keine Rechtsgrundlage“ anlässlich ihrer 77. Konferenz im März 2009 formulierten.

20 Rechtspflege

20.1 Allgemeines

Die im September 2008 festgestellte rechtswidrige Praxis der Videoüberwachung im Justizzentrum Magdeburg (vgl. IX. Tätigkeitsbericht, Nr. 19.4) hat das Justizministerium veranlasst, Handlungsanweisungen für den Umgang mit dem Datenschutz in der Justiz herauszugeben, mit deren Erstellung Herr Prof. Dr. Abel beauftragt wurde. Im November 2010 wurde dem Landesbeauftragten vom Justizministerium der schon für das Jahr 2009 avisierte Entwurf einer „Handreichung für den Datenschutz in der Justiz des Landes Sachsen-Anhalt“ übersandt. Sie kann eine Orientierung bei der Anwendung datenschutzrechtlicher Vorschriften bieten, deren Einhaltung der Landesbeauftragte zu überprüfen hat. Obwohl der Landesbeauftragte frühzeitig seine Bereitschaft erklärt hatte, an dem Prozess mitzuwirken und dies von der Landesregierung ausdrücklich begrüßt worden war, ist er nicht an der Erstellung der inhaltlichen Aussagen beteiligt worden. Die Handreichung lag auch im August 2011 noch nicht vor.

Unabhängig davon wirft die Handreichung auch einige grundsätzliche Fragen auf. So ist ihr nicht hinreichend zu entnehmen, in welchem Verhältnis sie zu den Verwaltungsvorschriften zum DSG-LSA steht. Auch ist nicht ersichtlich, ob die Justizvollzugsanstalten in den Anwendungsbereich einbezogen sind.

Erneut erweist sich auch in diesem Berichtszeitraum die Auftragsdatenverarbeitung in der Justiz als ein Dauerthema (vgl. IX. Tätigkeitsbericht, Nr. 19.1). Entweder wird zunächst nicht erkannt, dass es sich um Auftragsdatenverarbeitung handelt oder es wird den Anforderungen an eine ordnungsgemäße Auftragsdatenverarbeitung nicht Rechnung getragen (vgl. auch Nrn. 24.1 und 24.3). Deshalb ist noch einmal darauf hinzuweisen, dass im Regelfall Auftragsdatenverarbeitung vorliegt, wenn sich die Justiz bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines (weisungsabhängigen) Dritten bedient: Klassisches Beispiel sind hier die Verträge über die Entsorgung von Datenträgern. In diesen Konstellationen ist sie nach § 8 Abs. 6 DSG-LSA als Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten für den Datenschutz entsprechend den §§ 22 bis 24 DSG-LSA unterwirft. In dem Vertrag müssen insbesondere die Rechte und Pflichten des Auftraggebers nach dem DSG-LSA (z. B. Weisungsrechte und Überwachungspflichten) sowie die Rechte und Pflichten des Auftragnehmers nach dem DSG-LSA (Pflichten zur Datenverarbeitung, Dokumentation und Kennzeichnung, Unterwerfung unter die Weisungsbefugnis des Auftraggebers etc.) geregelt sein. Der Vertrag muss vorsehen, dass diese Rechte und Pflichten in Unterauftragsverhältnissen weitergegeben werden. Zudem ist sicherzustellen, dass die Justiz ihren Pflichten zur Überwachung des Auftragnehmers tatsächlich nachkommt.

20.2 Quellen-Telekommunikationsüberwachung

Hinter dem Begriff der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) verbirgt sich eine noch junge staatliche Überwachungsmaßnahme, die in einer gewissen Nähe zur Online-Durchsuchung steht: Die heimliche Überwachung von Telefonaten über das Internet.

Telefongespräche werden heute nicht nur über einen „normalen“ Telefonanschluss, sondern über den Computer oder das Mobiltelefon via Internet geführt. Die Sprachübertragung erfolgt dabei im Wege eines Voice-over-IP (VoiP)-Verfahrens mittels des Internet-Protokolls. Dabei enthalten die gängigen VoiP-Produkte eine Software, die die zu übermittelnden Audiodaten vor der Übertragung verschlüsselt. Bei einer herkömmlichen Telefonüberwachung werden daher nur verschlüsselte Daten abgefangen. Sie sind in Unkenntnis des Schlüssels wertlos. In der Praxis behilft man sich durch einen „Zugriff an der Quelle“, also am Endgerät des Kommunikationsteilnehmers. Dadurch wird auf die Daten zugegriffen, bevor sie verschlüsselt bzw. nachdem sie entschlüsselt wurden. Auf dem Computer des Betroffenen wird dazu eine speziell entwickelte Software installiert, die – wie ein Trojaner – die später abgehenden und ankommenden Gesprächsinhalte noch vor ihrer Verschlüsselung unbemerkt digital aufzeichnet und an die Behörden weiterleitet. Die Quellen-TKÜ setzt daher einen verdeckten Eingriff in ein informationstechnisches System, also in das vom Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung geschaffene neue Computergrundrecht, voraus (zu dieser Entscheidung siehe ausführlich Nr. 18.3 des IX. Tätigkeitsberichts).

Da die Quellen-TKÜ somit aus einer Kombination aus Telekommunikationsüberwachung und verdecktem Eingriff in ein informationstechnisches System besteht, stellt sich die Frage, ob der Eingriff nach dem für die Telekommunikationsüberwachung geltenden Maßstab des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG oder den vom Bundesverfassungsgericht für das neue Computergrundrecht geschaffenen Maßstäben zu beurteilen ist. In seinem Urteil zur Online-Durchsuchung hat das Bundesverfassungsgericht diese Frage dahingehend beantwortet, dass Art. 10 Abs. 1 GG der alleinige Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ ist, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt (NJW 2008, 826). Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein. Wird also mehr als der laufende Kommunikationsvorgang überwacht, gelten die Maßstäbe des neuen Computergrundrechts.

Die präventiv-polizeiliche Quellen-TKÜ war bisher im Polizeirecht des Bundes und der Länder nicht geregelt. Angesichts der Rechtsprechung des Bundesverfassungsgerichts haben der Bund mit § 20l BKAG, Bayern, Rheinland-Pfalz und Thüringen in ihrem Polizeirecht eine Rechtsgrundlage für die Quellen-TKÜ geschaffen. Die Vorschriften sehen im Wesentlichen vor, dass die Polizei die laufende Telekommunikation in der Weise überwachen und aufzeichnen kann, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und der Eingriff in das informations-

technische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

Die Strafprozessordnung (StPO) enthält dagegen bisher keine Regelung, die den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts gerecht wird. Dennoch will ein Teil der Rechtsprechung und Lehre die Quellen-TKÜ auf der Rechtsgrundlage der für die herkömmliche Telekommunikationsüberwachung geschaffenen §§ 100a, 100b StPO zulassen. Gerechtfertigt wird dies im Wesentlichen damit, dass der Richter im Rahmen der Anordnung der Telekommunikationsüberwachung nach § 100b Abs. 2 Satz 2 Nr. 3 StPO die rechtlichen und technischen Vorgaben für die Telekommunikationsüberwachung treffe und dadurch sicherstelle, dass sich die Überwachung ausschließlich auf den laufenden Telekommunikationsvorgang beschränke. Im grundrechtsrelevanten Bereich kann der Gesetzgeber jedoch nicht durch den Richter ersetzt werden. Vielmehr muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Daher müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Wie problematisch die Quellen-TKÜ sein kann, zeigt folgender von dem Nachrichtenmagazin Spiegel in seiner Ausgabe 9/2011 geschilderter Fall, der sich in ähnlicher Weise in jedem Bundesland, also auch in Sachsen-Anhalt, hätte ereignen können. Danach installierte das bayerische Landeskriminalamt auf dem Laptop eines Geschäftsmannes im Rahmen einer Routinekontrolle im Flughafen München wegen des Verdachts des banden- und gewerbemäßigen Handelns mit Betäubungsmitteln eine Spionagesoftware, die nicht nur den laufenden Telekommunikationsvorgang überwachte, sondern alle 30 Sekunden ein Foto des Bildschirms aufnahm und die Aufnahmen an das Landeskriminalamt versendete. Der Amtsrichter hatte diese sog. Screenshots für rechtmäßig gehalten. Erst das mit dieser Sache befasste Landgericht stellte fest, dass das Kopieren und Speichern der grafischen Bildschirminhalte rechtswidrig ist, weil zum Zeitpunkt dieser Maßnahmen noch kein Telekommunikationsvorgang stattfindet.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher den Gesetzgeber aufgefordert, Rechtssicherheit – gerade für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären (Entschließung der 81. Konferenz der Datenschutzbeauftragten vom März 2011: „Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten“, **Anlage 20**).

Die neue Landesregierung will in der 6. Legislaturperiode den Verfassungsschutz zu einer präventiven Quellen-Telekommunikationsüberwachung ermächtigen. Das betrachtet der Landesbeauftragte grundskeptisch.

20.3 Vorratsdatenspeicherung

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nrn. 19.2 und 24.1) bereits seine Bedenken gegen die Vorratsdatenspeicherung dargestellt

und berichtet, dass das Bundesverfassungsgericht mit Beschluss vom 11. März 2008 eine einstweilige Anordnung erlassen hatte, nach der § 113b Satz 1 Nr. 1 TKG bis zur Entscheidung in der Hauptsache nur eingeschränkt angewendet werden durfte (vgl. BVerfGE 121, 1). Mit Beschluss vom 28. Oktober 2008 hat das Gericht diese einstweilige Anordnung dahingehend erweitert, dass auch von § 113b Satz 1 Nrn. 2 und 3 TKG bis zur Hauptsacheentscheidung nur mit Einschränkungen Gebrauch gemacht werden konnte (vgl. BVerfGE 122, 120).

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht seine Rechtsprechung im Ergebnis bestätigt (BVerfGE 125, 260; NJW 2010, 833). Es hat entschieden, dass die Regelungen des TKG und des § 100g StPO, der in Konkretisierung des § 113b Satz 1 Nr. 1 TKG die unmittelbare Verwendung der vorsorglich gespeicherten Daten für die Strafverfolgung regelt, mit Art. 10 Abs. 1 GG nicht vereinbar sind. Zwar ist eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehlt aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hinreichende Datensicherheit noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügen sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz- und Rechtsschutzanforderungen. Die Regelung ist damit insgesamt verfassungswidrig und nichtig. Ob bzw. in welchem Umfang die Vorratsdatenspeicherung neu geregelt werden soll, ist innerhalb der Bundesregierung umstritten. Zu den Einzelheiten des Urteils des Bundesverfassungsgerichts und der weiteren politischen Entwicklung auf europäischer und nationaler Ebene wird wegen des engeren Sachzusammenhangs auf den Beitrag zum Telekommunikations- und Medienrecht unter Nr. 25.1 verwiesen (vgl. im Übrigen zur Frage der Verwertbarkeit von vor dem Urteil und nach dem Beschluss vom 11. März 2008 erhobenen Daten: BGH, Beschlüsse vom 13. und 18. Januar 2011, NJW 2011, 1827 und 1377).

20.4 Justizaktenaufbewahrung

In seinem IX. Tätigkeitsbericht (Nr. 19.8) hatte der Landesbeauftragte berichtet, dass Sachsen-Anhalt für die Justiz ein Schriftgutaufbewahrungsgesetz (JSchrG LSA; GVBl. LSA 2008 S. 236) erlassen hat. Im Berichtszeitraum lag jedoch die nach § 2 JSchrG LSA zu erlassende Ausführungsverordnung noch nicht vor. Die Verordnung zur Ausführung des Gesetzes zur Aufbewahrung von Schriftgut der Gerichte der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften, der Justizvollzugsbehörden und des Sozialen Dienstes der Justiz des Landes Sachsen-Anhalt (AufbewahrungsVO LSA) wurde im Juni 2009 erlassen (GVBl. LSA 2009 S. 264) und zuletzt im März 2010 (GVBl. LSA S. 157) noch einmal geändert.

20.5 Zwangsversteigerung und Internet

In seinem IX. Tätigkeitsbericht (Nr. 19.10) hatte der Landesbeauftragte berichtet, dass im Rahmen eines Zwangsversteigerungsverfahrens ein gerichtlich beauftragter Gutachter Bilder von der Wohnung des Petenten ohne dessen Einverständnis ins Internet eingestellt hatte. Der Landesbeauftragte hatte diese Vorgehensweise für bedenklich gehalten, da aus den eingestellten Bildern Rückschlüsse auf die Person hätten getroffen werden können. Er hatte

daher das Justizministerium um Stellungnahme gebeten, die im Berichtszeitraum noch nicht vorlag.

In der Stellungnahme, die dem Landesbeauftragten erst im Berichtszeitraum des X. Tätigkeitsberichts zuging, teilte das Justizministerium mit, dass es sich bei dem angesprochenen Verfahren um einen bedauerlichen Einzelfall gehandelt haben dürfte.

Die Landesregierung hat in ihrer Stellungnahme zum IX. Tätigkeitsbericht unter Bezugnahme auf die Antwort des Justizministeriums darauf verwiesen, dass die Internetveröffentlichung von Gutachten – auch unter Einbeziehung privater Anbieter – in Zwangsversteigerungsverfahren bundesweit die Regel sei und hierfür auf §§ 38 Abs. 2, 39 Abs. 1 und 40 Abs. 2 ZVG zurückgegriffen werde. Zur Veröffentlichung gelangten überarbeitete und anonymisierte Exemplare, um den schutzwürdigen Interessen der Betroffenen Rechnung zu tragen.

Ergänzend ist anzumerken, dass der Bundesgesetzgeber mit dem Gesetz über die Internetversteigerung in der Zwangsvollstreckung vom 29. Juli 2009 (BGBl. I S. 2258/2269) durch eine Modifizierung der §§ 814 ff. ZPO die Internetversteigerung neben der Präsenzversteigerung vor Ort durch den Gerichtsvollzieher zum Regelfall gemacht hat. Die Bundesländer wurden darüber hinaus gem. § 814 Abs. 3 ZPO ermächtigt, Einzelheiten wie etwa die Versteigerungsplattform, Beginn, Ende und Ablauf der Aktion oder die Voraussetzungen für die Teilnahme an der Versteigerung durch Rechtsverordnung zu regeln.

Das Ministerium der Justiz hat zuletzt mit der Ausführungsvorschrift vom 24. März 2010 bestimmt, dass die nach §§ 39 Abs. 1, 38 Abs. 2 ZVG vorgeschriebene öffentliche Bekanntmachung unter der Internet-Adresse http://www.zvg-portal.de veröffentlicht wird. Hierbei handelt es sich um das von den Landesjustizverwaltungen geschaffene Portal zur Information über Zwangsversteigerungsverfahren.

20.6 Fragebogen zur Zulassung zur Rechtsanwaltschaft

Anlässlich einer Eingabe beim Bayerischen Landesbeauftragten für den Datenschutz diskutierte der Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, ob die von den Rechtsanwaltskammern verwandten Fragebögen zum Antrag auf Zulassung zur Rechtsanwaltschaft den datenschutzrechtlichen Anforderungen genügen. Da der Fragebogen der Rechtsanwaltskammer Sachsen-Anhalt mit dem im vorliegenden Fall maßgeblichen Fragebogen der Rechtsanwaltskammer München identisch war, hat der Landesbeauftragte das zuständige Justizministerium zu den problematischen Auskunftsverlangen um Stellungnahme gebeten.

So verlangte der Fragebogen von dem Bewerber Auskunft über die Verhängung strafgerichtlicher Verurteilungen. Während getilgte Verurteilungen nicht mehr angegeben werden sollten, bestand für tilgungsreife Verurteilungen noch eine Auskunftspflicht. Nachdem der Landesbeauftragte das Justizministerium darauf hingewiesen hat, dass nach § 51 Abs. 1 BZRG auch tilgungsreife Verurteilungen dem Betroffenen im Rechtsverkehr nicht zum Nachteil

gereichen dürfen, soll der Fragebogen geändert werden. Zu tilgende Verurteilungen sind zukünftig nicht mehr anzugeben.

Ferner soll ein Bewerber nun nur noch angeben müssen, ob er zum Zeitpunkt der Antragstellung Beamter, Richter oder Soldat auf Zeit ist, da nur in diesem Fall die Zulassung zur Rechtsanwaltschaft versagt werden kann. Es soll daher nicht mehr danach gefragt werden, ob der Bewerber diesen Beruf zu einem früheren Zeitpunkt ausgeübt hat.

Beibehalten wurde dagegen die Frage nach anhängigen oder anhängig gewesenen Straf-, Disziplinar- oder anwaltsgerichtlichen Verfahren gegen den Bewerber. Dieser muss also weiterhin die o. g. Verfahren angeben, auch wenn sie gem. § 170 Abs. 2 StPO wegen Schuldunfähigkeit oder Vorliegen eines Verfahrenshindernisses, §§ 153, 153a bis f, 154a bis e StPO vorläufig oder endgültig eingestellt wurden. Der Landesbeauftragte hatte darauf hingewiesen, dass viele der in den Vorschriften zur Verfahrenseinstellung genannten Verhaltensweisen grundsätzlich nicht geeignet seien, einen Bewerber für den Anwaltsberuf untragbar erscheinen zu lassen. So sei z. B. nicht nachvollziehbar, warum ein Bewerber bei einer Verfahrenseinstellung wegen geringer Schuld nach § 153 StPO nicht würdig sein solle, den Beruf des Rechtsanwalts auszuüben. Das Justizministerium hat seine Auffassung im Wesentlichen damit begründet, dass die Erfassung des in Frage stehenden Verhaltens erforderlich sei, um im Rahmen einer Gesamtschau die Geeignetheit des Zulassungsbewerbers würdigen zu können. Gerade im Kontext mit anderen Vorfällen könnte sich im Einzelfall eine Unwürdigkeit des Bewerbers ergeben. Im Ergebnis erscheint diese Auffassung vertretbar.

20.7 Einsatz externer Gutachter im Kampf gegen Kinderpornographie

Im März 2010 erlangte der Landesbeauftragte durch Presseberichte davon Kenntnis, dass das Justizministerium in Abstimmung mit der „Zentralstelle gegen Kinderpornographie“ bei der Staatsanwaltschaft Halle beabsichtigt, externe Gutachter mit der Auswertung beschlagnahmter Computer, Mobiltelefone und sonstiger Speichermedien zu beauftragen. Hintergrund der Überlegungen sei eine Entscheidung des Landgerichtes Magdeburg aus dem Sommer 2009. Das Gericht hat die Behörden angewiesen, Beweismittel an einen des Besitzes kinderpornographischer Darstellungen Verdächtigen zurückzugeben, weil beschlagnahmte Speichermedien nicht unbegrenzt einbehalten werden dürfen. Diese Entscheidung setzt die Ermittlungsbehörden bei der Auswertung von Daten unter einen gewissen zeitlichen Druck.

Auf die entsprechende Anfrage durch den Landesbeauftragten wurde ihm das Muster eines Gutachtens eines externen Gutachters zur forensischen Auswertung von Datenträgern übersandt. So konnte sich der Landesbeauftragte ein Bild davon machen, welchen Umfang die durch externe Gutachter zur Kenntnis genommenen personenbezogenen Daten der Betroffenen annehmen können.

Die Auswertung beschlagnahmter Datenträger in der in Sachsen-Anhalt vorgesehenen Weise erscheint datenschutzrechtlich vertretbar. Zwar bestehen zum einen Bedenken hinsichtlich der Zulässigkeit aufgrund der Regelungen des § 110 StPO. Danach steht die Durchsicht der Papiere der Staatsanwalt-

schaft und auf deren Anordnung deren Ermittlungspersonen – der Polizei – zu. Die Übertragung ihrer Kompetenz an private Dritte ist nicht vorgesehen. Selbstverständlich ist die Hinzuziehung von Sachverständigen zulässig, allerdings setzt dies voraus, dass eine Sichtung des Materials vorgenommen wurde, um so die Notwendigkeit einer sachverständigen Begutachtung beurteilen zu können. Entsprechend argumentierte das Landgericht Kiel in seiner Entscheidung vom 14. August 2006 (Az.: 37 Qs 54/06, NJW 2006, 3224), das im konkreten Fall die zu selbstständige Bearbeitung des Sachverständigen rügte. Andererseits sieht Sachsen-Anhalts Justizministerin keine Probleme. In der Presse wird sie zitiert: „Nachfragen in anderen Bundesländern, in denen Fremdvergabe bereits praktiziert wird, haben ergeben, dass es damit durchaus positive Erfahrungen gibt." Privatfirmen sollen nur dort herangezogen werden, wo die Frist, in denen eine Auswertung zu erfolgen hat, abzulaufen droht. Die unter Anleitung der Staatsanwaltschaft stehenden neutralen Sachverständigen wahren die Datensicherheit der überlassenen Datenspeicher. Von „privaten Ermittlern" kann nicht die Rede sein.

20.8 Hypnose im Ermittlungsverfahren

Der Fachliteratur sowie der Presse ließ sich entnehmen, dass die forensische Hypnose als erinnerungsunterstützendes Verfahren bei Aussagen von Zeugen und Opfern im Ermittlungsverfahren mit steigender Tendenz zur Anwendung kommt. Zuletzt hatte die Presse im Mai 2008 berichtet, dass in Bayern auf Veranlassung der Strafverfolgungsbehörden in zwei Fällen Hypnosesitzungen mit Zeugen durchgeführt wurden. Die Zeugen sollten sich an das Kennzeichen eines Kraftfahrzeugs erinnern, das vermutlich bei der Begehung von Straftaten verwandt worden war. Da es sich um ein neueres Verfahren handelt, war die Rechtmäßigkeit dieser Maßnahme Gegenstand des Arbeitskreises Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Nach § 136a StPO gehört die Anwendung der Hypnose bei der Vernehmung von Zeugen oder Beschuldigten zu den verbotenen Vernehmungsmethoden. Diese dürfen daher auch bei Vorliegen einer Einwilligung des Betroffenen nicht angewandt werden. Das bayerische Staatsministerium der Justiz und für Verbraucherschutz vertritt allerdings die Auffassung, dass ein Zeuge auf Initiative der Ermittlungsbehörden sich einer Hypnose unterziehen und das Ergebnis den Ermittlungsbehörden mitteilen dürfe. Das Ministerium hat seine Auffassung im Wesentlichen damit begründet, dass es sich nicht um eine verbotene Vernehmungsmethode handele, da die Hypnose dann außerhalb einer Vernehmungssituation erfolge. Diese Auffassung hat der bayerische Landesbeauftragte als unzutreffend zurückgewiesen. Ausschlaggebend sei, dass der Einsatz auf Initiative der Ermittlungsbehörden erfolge und ihr damit auch als eigene Maßnahme zuzurechnen sei.

Vor diesem Hintergrund hat der Landesbeauftragte die ihm aus Bayern bekannt gewordene Praxis zum Anlass genommen, sich bei den zuständigen Ministerien der Justiz und des Inneren über die Rechtspraxis in Sachsen-Anhalt zu informieren. Das Justizministerium hat ihm daraufhin mitgeteilt, dass es den Einsatz von Hypnose zur Aufklärung von Straftaten im Ermittlungsverfahren für unzulässig halte. Dies gelte auch für die Vernehmung von Zeugen außerhalb einer konkreten Vernehmungssituation, die allein auf Ver-

anlassung der Ermittlungsbehörden erfolge. Korrespondierend dazu ergab die Anfrage beim Innenministerium, dass in Sachsen-Anhalt die Polizei die Hypnose im Ermittlungsverfahren bisher nicht eingesetzt hat.

20.9 Straftäterüberwachung mittels Global Positioning System

Am 2. September 2010 hat der Europäische Gerichtshof für Menschenrechte in Straßburg bestätigt, dass der Einsatz von GPS (Global Positioning System) bei deutschen Ermittlungsverfahren nicht gegen die Europäische Menschenrechtskonvention verstößt (Individualbeschwerde Nr. 35623/05, NJW 2011, 1333).

Der Entscheidung vorausgegangen war ein jahrelanger Rechtsstreit. Dem Beschuldigten wurde vorgeworfen, an Sprengstoffanschlägen beteiligt gewesen zu sein.

Da der Beschuldigte zu dieser Zeit bereits mehrfach wegen politisch motivierten Straftaten vorbestraft war und im Verdacht stand, Mitglied einer linksextremistischen terroristischen Vereinigung zu sein, wurde er durch Mitarbeiter des Verfassungsschutzes observiert. Die Maßnahmen schlossen eine Video- und Telefonüberwachung mit ein. Letztlich wurde außerdem das von dem Beschuldigten genutzte Fahrzeug mit einem GPS-Modul ausgerüstet, welches Datum, Uhrzeit, die geographischen Breiten- und Längenkoordinaten sowie die Geschwindigkeit des Fahrzeugs aufzeichnete.

Der Beschuldigte wurde durch das Oberlandesgericht Düsseldorf zu einer Freiheitsstrafe von 13 Jahren verurteilt. Das Gericht zog bei seiner Beurteilung auch die Daten der GPS-Überwachung als Beweismittel heran.

Der Bundesgerichtshof bestätigte mit Urteil vom 24. Januar 2001 (Az.: 3 StR 324/00, NJW 2001, 1658) das Urteil des Oberlandesgerichts Düsseldorf. Die Gewinnung von Beweisen unter Verwendung des GPS war gemäß § 100c Abs. 1 Nr. 1b StPO (alte Fassung, heute § 100h StPO) zulässig. Hiernach gehört das GPS zu den sonstigen für Observationszwecke bestimmten technischen Mitteln, und der unantastbare Kernbereich der Privatsphäre wurde nicht berührt. Bei diesem erheblichen, verfassungsrechtlich anerkannten Interesse an der Straftatsaufklärung handelt es sich um eine durch einen Gesetzesvorbehalt gedeckte Grundrechtseinschränkung.

Die eingelegte Verfassungsbeschwerde hatte ebenfalls keinen Erfolg. Das Bundesverfassungsgericht entschied mit Urteil vom 12. April 2005 (Az.: 2 BvR 581/01, NJW 2005, 1338), dass § 100c Abs. 1 Nr. 1b StPO (alter Fassung) als Ermächtigungsgrundlage für Beweiserhebungen unter Einsatz des GPS den verfassungsrechtlichen Anforderungen entspricht. Jedoch wies das Bundesverfassungsgericht auch darauf hin, dass auf Grund der schnellen Entwicklung der Technik der Gesetzgeber die technischen Entwicklungen beobachten und notfalls durch ergänzende Rechtsetzung korrigierend eingreifen muss (vgl. Nr. 1.1).

Daraufhin wandte der Beschwerdeführer sich an den Europäischen Gerichtshof für Menschenrechte. Auch hier rügte der Beschwerdeführer den

Eingriff in sein Recht auf Achtung seines Privatlebens (Art. 8 der Europäischen Menschenrechtskonvention).

Der Europäische Gerichtshof für Menschenrechte stellte klar, dass die Überwachung mittels GPS eine Maßnahme nach § 100c Abs. 1 Nr. 1b StPO (alte Fassung) darstelle. Auch die Verhältnismäßigkeit der GPS-Überwachung wurde durch das Gericht bestätigt, da sie nicht von Anfang an als Überwachungsmaßnahme angeordnet war, sondern erst nachdem andere Maßnahmen fehlschlugen. Eine weitere wichtige Rolle spielte die Schwere der Straftaten, wegen der ermittelt wurde, in diesem Fall versuchter Mord durch Sprengstoffexplosionen. Somit ist Art. 8 der Europäischen Menschenrechtskonvention nicht verletzt worden.

20.10 Reality-TV

In den letzten Jahren haben sog. Reality-TV-Produktionen im Justiz-, Polizei- und Sozialbereich, bei denen staatliche Stellen dem Fernsehen die Möglichkeit geben, Amtsträger bei der Arbeit zu begleiten und Filmaufnahmen zu fertigen, erheblich zugenommen. Berichtet wird somit über echte Personen und Fälle, die Gegenstand behördlichen Handelns geworden sind, von der Zwangsvollstreckung, der Lebensmittelüberwachung bis hin zur Verkehrskontrolle. Presse- und Öffentlichkeitsarbeit der Behörden sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und dem Informationsanspruch der Öffentlichkeit Genüge zu tun. Ziel der Reality-TV-Formate ist jedoch zumeist nicht eine sachliche Information der Bevölkerung, vielmehr stehen die Unterhaltung und Befriedigung der Sensationslust des Publikums im Vordergrund, denn durch die gezeigten staatlichen Maßnahmen werden die Betroffenen nicht selten bloßgestellt.

Die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 darauf hingewiesen, dass es sich rechtlich um eine Datenübermittlung an private Dritte handelt, wenn Behörden das Fernsehen in die Lage versetzen, personenbezogene Filmaufnahmen anzufertigen. Für einen solchen massiven Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung der behördlichen Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Mangels Rechtsgrundlage sind solche Berichte daher nur zulässig, wenn der Betroffene vorher in die Berichterstattung eingewilligt hat. Dafür ist es notwendig, die betroffenen Personen rechtzeitig über Umfang, Dauer und Verwendungszweck der Aufnahmen aufzuklären und auf die Freiwilligkeit der Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Konferenz der Datenschutzbeauftragten hat daher in ihrer Entschließung „Reality-TV – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen“ (**Anlage 6**) die Behörden aufgefordert, von der Mitwirkung an solchen „Reality-Reportagen“ Abstand zu nehmen.

In diesem Zusammenhang ist auf eine weitere Entscheidung des Bundesverfassungsgerichts vom 14. September 2010, die die Berichterstattung in Wort

und Ton über eine Tochter von Caroline von Monaco betraf, zu verweisen. Danach reicht der Schutz des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 GG i. V. m. Art. 1 GG hinsichtlich der Veröffentlichung von Bildern und der Berichterstattung durch Wortbeiträge unterschiedlich weit (NJW 2011, 740). Während die Veröffentlichung eines Bildes einer Person grundsätzlich eine rechtfertigungsbedürftige Beschränkung ihres allgemeinen Persönlichkeitsrechts begründet, die unabhängig davon ist, ob die Person in privaten oder öffentlichen Zusammenhängen und in vorteilhafter oder unvorteilhafter Weise abgebildet ist, ist dies bei personenbezogenen Wortberichten nicht ohne Weiteres der Fall. Artikel 2 Abs. 1 GG bietet hier nicht schon davor Schutz, überhaupt in einem Bericht individualisierend genannt zu werden, sondern nur in spezifischen Hinsichten. Dabei kommt es vor allem auf den Inhalt der Berichterstattung an. Das allgemeine Persönlichkeitsrecht schützt insbesondere vor der Beeinträchtigung der Privat- und der Intimsphäre, des Weiteren vor herabsetzenden oder ehrverletzenden Äußerungen oder davor, dass einem Betroffenen Äußerungen zugeschrieben werden, die er gar nicht getätigt hat.

20.11 Beschlagnahme von E-Mails beim Provider nicht verfassungswidrig

Nach einem Beschluss des Bundesverfassungsgerichts vom 16. Juni 2009 (NJW 2009, 2431) können E-Mails bei strafprozessualen Ermittlungsverfahren der Polizei auch dann beschlagnahmt werden, wenn sie auf dem E-Mail-Server des Providers zwischen- oder endgespeichert sind. Dabei müssen die strengen Voraussetzungen einer Telefonüberwachung gem. § 100a StPO nicht erfüllt sein. Die Ermittler können sich auf die Regelungen zur Beschlagnahme (§§ 94 ff. StPO) stützen. Allerdings unterliegen auch die gespeicherten E-Mails dem Schutz des Fernmeldegeheimnisses, sodass bei einer Beschlagnahme genau geprüft werden muss, ob der Eingriff in die Rechte des Betroffenen verhältnismäßig ist. Der effektive Schutz von Art. 10 Abs. 1 GG bedarf zudem einer den sachlichen Erfordernissen entsprechenden Ausgestaltung des Verfahrens.

Mit dieser Entscheidung wurde eine Verfassungsbeschwerde abgewiesen, die sich gegen die Sicherstellung und Beschlagnahme von E-Mails auf dem E-Mail-Server eines Providers richtete. Im Zuge von Ermittlungen wegen Betrugs und Untreue war die Wohnung des Beschwerdeführers durchsucht worden, um Unterlagen, Datenträger und insbesondere Textdateien und E-Mails zu finden, die als Beweismittel dienen könnten. Da sich die E-Mails auf dem E-Mail-Server seines Providers befanden, verwahrte sich der Beschwerdeführer gegen den Zugriff auf diese E-Mails. Daraufhin ordnete das Amtsgericht die Beschlagnahme der E-Mails beim Provider an.

Da es den Ermittlern nicht möglich war, die E-Mails nach ihrer Relevanz für das Verfahren vor Ort zu sortieren, wurden die gesamten ca. 2.500 E-Mails des Beschwerdeführers kopiert. Nach Ansicht des Gerichts ist eine vorläufige Sicherstellung größerer Teile oder des gesamten E-Mail-Bestandes zulässig. Allerdings muss sichergestellt werden, dass bei der anschließenden Durchsicht Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist.

Vor der Sicherstellung von E-Mails, die in einem Postfach auf dem E-Mail-Server des Providers gespeichert sind, ist im Regelfall der Postfachinhaber von den Strafverfolgungsbehörden zu unterrichten, damit er bei der Sichtung seines E-Mail-Bestandes seine Rechte wahrnehmen kann. Werden E-Mails ausnahmsweise ohne Wissen des Postfachinhabers sichergestellt, ist dieser so früh, wie es die wirksame Verfolgung des Ermittlungszwecks erlaubt, darüber zu unterrichten. Diesen Anforderungen wird durch §§ 35 und 98 Abs. 2 Satz 5 StPO Rechnung getragen.

21 Schulen

21.1 Soziale Netzwerke

Im IX. Tätigkeitsbericht (Nr. 20.5) hatte der Landesbeauftragte auf Gefährdungen der Privatsphäre durch die Teilnahme und das Eingeben von Daten in sozialen Netzwerken hingewiesen. Der Kreis der Nutzer nimmt gigantische Ausmaße an. Betrachtet man Datenschutz auch als Bildungsaufgabe, ist es weiter geboten, die sich aus der Nutzung dieses modernen Kommunikations- und Präsentationsinstruments ergebenden Risiken zu beobachten und auf mehr Medienkompetenz hinzuwirken. Das beinhaltet Wissens-, aber stets auch Wertevermittlung.

Die Entwicklungen im Bereich der sozialen Netzwerke, die sich regelmäßig der Medienberichterstattung entnehmen lassen, zeigen die Berechtigung der Forderungen der Datenschützer auf. Immer wieder erscheinen Meldungen zur Praxis von sozialen Netzwerken, die mit umfänglichen Transfers von Daten überraschen. Oft wird auch über Vorfälle berichtet, in denen der unberechtigte Zugang zu vermeintlich geschützten Daten in großem Umfang erfolgte.

Es ist eine erhöhte Transparenz geboten, den Betroffenen muss der Schutz ihrer Privatsphäre erleichtert werden. Zwar besteht eine grundsätzliche Bindung an gesetzliche Vorgaben. Doch wird auch einem Mitglied der Bundesregierung die Äußerung zum Branchenprimus zugeschrieben, dass die Bundesregierung eine solche Firma nicht regulieren könne.

Zum erheblichen Schutz-, Aufklärungs- und Informationsbedarf haben auch die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im November 2010 den Beschluss „Minderjährige in sozialen Netzwerken wirksamer schützen“ gefasst (**Anlage 25**).

Der Bundesrat beschloss auf Initiative Hessens einen Gesetzentwurf zur Änderung des Telemediengesetzes (BR-Drs. 156/11 (Beschluss) vom 17. Juni 2011), um die Transparenz und die Nutzerrechte bei sozialen Netzwerken zu stärken. Die Bundesregierung steht dem Vorhaben eher skeptisch gegenüber und verweist auf Klärungsbedarf auf EU-Ebene (BT-Drs. 17/6765).

21.2 Medienkompetenz und Datenschutzbewusstsein

Der Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auch in diesem Berichtszeit-

raum die Vernetzung der verschiedenen Beteiligten auf Länder- und Bundesebene forciert.

In Sachsen-Anhalt hat der Landtag am 10. September 2010 beschlossen (LT-Drs. 5/89/2614 B), dass die Landesregierung ein Konzept für die Stärkung der Medienkompetenz erarbeiten und in den Ausschüssen für Bundes- und Europaangelegenheiten sowie Medien und für Bildung, Wissenschaft und Kultur vorstellen soll. Das Kultusministerium hat das Konzept mit Schreiben vom 4. Februar 2011 vorgelegt. Die Ausschüsse haben das Konzept zur Kenntnis genommen. Der Landesbeauftragte hatte bereits im Juni 2010 ausführlich im Bildungsausschuss über die Situation im Bereich der Vermittlung von Medienkompetenz im Land und darüber hinaus über Ansätze und Defizite, Akteure und Angebote berichtet und Erwartungen und Forderungen formuliert. Seitens des Kultusministeriums wäre ein aktiveres, intensiveres Vorgehen geboten, auch angesichts von Vorbildern in anderen Ländern.

Das Konzept soll als Grundlage für einen konkreten Maßnahmenplan zur Stärkung der Medienkompetenz und Förderung der Medienbildung dienen. Bei der Erstellung des Konzeptes wurden neben dem Landesbeauftragten u. a. auch die Medienanstalt, das Landesinstitut für Schulqualität und Lehrerbildung, der Lehrstuhl für Medien- und Erwachsenenbildung am Institut für Erziehungswissenschaft der Otto-von-Guericke-Universität Magdeburg und die Landeszentrale für politische Bildung beteiligt. Betrachtet werden im Konzept die Bereiche der vorschulischen und schulischen Bildung, aber auch die Medienkompetenz im Alltag, der Datenschutz, der Jugendmedienschutz und die privaten und öffentlichen Medienanbieter. Als konkrete Maßnahmen werden u. a. die bessere Vernetzung der Beteiligten und die Errichtung einer Arbeitsgemeinschaft „Medienbildung/-kompetenz Sachsen-Anhalt“ festgelegt. Der Landesbeauftragte ist ständiges Mitglied dieser Arbeitsgemeinschaft und wird auch in diesem Rahmen eine weitergehende Förderung von Medienkompetenz und Datenschutzbewusstsein einfordern und daran mitwirken.

Inhaltlich betrachtet dürften neben der Schulausbildung und der Lehrerfortbildung auch die Lehrerausbildung, Erwachsenenbildung und Verbraucherbildung relevant sein.

Konkrete Vorschläge zielen auf die Ergänzung der Lehramtsstudiengänge und der Rahmenrichtlinien und Lehrpläne, Unterrichtsmodule im Sinne von Querschnittsinhalten (nicht auf bestimmte Fächer konzentriert), Medienberater auf Landkreisebene, Broschüren zum Thema Soziale Netzwerke, Medienkompetenzführerscheine, Einbeziehung externer Experten in die Unterrichte.

Die Thematik soll auf einer Netzwerktagung im September 2011 vertieft werden, an der der Landesbeauftragte mitwirkt. Es geht danach um eine breitere Vernetzung, multiplikatorische Strukturen, flächendeckende Angebote und verpflichtende Vorgaben, konzeptionelle nachhaltige Maßnahmen. Dabei wird mit der Komponente Datenschutz und Datenschutzbewusstsein als Kernkompetenz von Medienkompetenz eine besondere Wertevermittlung im Sinne von § 1 SchulG LSA vorzunehmen sein. Darauf wird auch bei der von der Kultusministerkonferenz beabsichtigten Empfehlung zur Medienbildung in der Schule zu achten sein.

21.3 Prüfung in Schulen

Auch in diesem Berichtszeitraum hat der Landesbeauftragte wieder Schulen hinsichtlich der Einhaltung der datenschutzrechtlichen Vorschriften geprüft.

Sowohl in einem Gymnasium als auch in einer Berufsbildenden Schule musste festgestellt werden, dass kein behördlicher Datenschutzbeauftragter nach § 14a DSG-LSA bestellt war, obwohl automatisierte Verfahren zur Datenverarbeitung verwendet werden. In beiden Fällen wurde dies unverzüglich nachgeholt, sodass von einer Beanstandung abgesehen werden konnte. Aufgrund der Dauer des Bestehens der Bestellungsverpflichtung (seit 2001) darf dies eigentlich nicht mehr vorkommen. Der Landesbeauftragte empfiehlt daher dringend allen Schulen in Sachsen-Anhalt zu prüfen, ob ein behördlicher Datenschutzbeauftragter nach § 14a DSG-LSA zu bestellen ist, und sofern dies erforderlich ist, sogleich die Bestellung vorzunehmen.

Darüber hinaus hat der Landesbeauftragte datenschutzrechtliche Hinweise bezüglich der Veröffentlichung von personenbezogenen Sportergebnissen, Projektteilnahmen u. ä. im Schulgebäude und im Internet gegeben. Eine Veröffentlichung dieser Daten ist nur auf der Grundlage einer Einwilligung des Betroffenen, die den Voraussetzungen des § 4 Abs. 2 DSG-LSA entspricht, zulässig.

21.4 Schulverwaltungssoftware

Der Aspekt der Erforderlichkeit der Datenhaltung für die konkrete Aufgabenerfüllung stand im Vordergrund der Beratungen des Landesbeauftragten zur Einführung einer einheitlichen Schulverwaltungssoftware. Zu den Darlegungen im IX. Tätigkeitsbericht (Nr. 20.3) nahm die Landesregierung dahingehend Stellung, dass der Landesbeauftragte weiter in die Entwicklung der Software einbezogen wird, seine Hinweise und Anregungen berücksichtigt werden und das Trennungsgebot von Verwaltung und Statistik besonders beachtet werde. Die Schulverwaltungssoftware solle der Verwaltungsvereinfachung dienen, zugleich aber auch der Umsetzung des Beschlusses der Kultusministerkonferenz aus dem Jahre 2003 zur Einführung eines bundeseinheitlichen Kerndatensatzes. Nach der Stellungnahme der Landesregierung zu Nr. 20.2 des IX. Tätigkeitsberichts (Kerndatensatz) sollen allerdings Daten für eine nationale Schülerdatenbank erst bereitgestellt werden, wenn dafür ein schlüssiges, mit den Landesbeauftragten für den Datenschutz abgestimmtes Konzept vorliegt.

Es fanden daher weitere Erörterungen mit dem Kultusministerium zur datenschutzgerechten Ausgestaltung von Regelungen und Verfahren statt, die die Aufgabenerfüllung der Schulbehörden sicherstellen und dabei der Datensparsamkeit Rechnung tragen soll.
Unter anderem sollen zur Vermeidung einer nicht unbeträchtlichen Anzahl von Doppelungen eine zentrale operative Datenbank entstehen, in Anlehnung an andere Länder Schüleridentifikationsnummern vergeben und schulübergreifende Plausibilitätsprüfungen durchgeführt werden. Für statistische Auswertungen soll durch technische Verfahren sichergestellt werden, dass ein Rückschluss aus den statistischen Daten ausgeschlossen ist.
Grundsätzlich bestehen die gesetzlichen Befugnisse, die die für die Erfüllung

von Verwaltungsaufgaben erforderliche Datenverarbeitung gestatten. Allerdings kann die Erforderlichkeit einer umfassenden zentralen Datei fraglich sein, wenn die Aufgaben anderweitig erledigt werden können. So könnten beispielsweise Mehrfachbewerbungen auch dadurch vermieden werden, dass wirksame Anmeldungen nur durch Vorlage des Originalzeugnisses möglich sind. Notwendig erscheint sicher, die aufwändige Neueingabe bei jährlich ca. 50.000 Schulwechseln zu vermeiden. Die Übermittlung der Schülerdaten von der abgebenden an die aufnehmende Schule könnte aber ggf. auch bilateral elektronisch im Zusammenhang mit der Abgabe der Schülerakten erfolgen, anstatt durch Einschaltung einer dritten, zentralen Stelle. Auch die Speicherdauer ist für die einzelnen Daten zu hinterfragen.
Angesichts der angedachten Dimension hat der Landesbeauftragte angeregt, ggf. wie in anderen Ländern eine differenzierte gesetzliche Grundlage hinsichtlich des Datenumfangs zu schaffen. Soweit über die grundlegende Schulverwaltung hinaus die Verwendung von Bildungsverlaufsdaten zu einzelnen Schülern zu Zwecken der Bildungsplanung vorgesehen ist, sollten die Verfahren, insbesondere zur sicheren Pseudonymisierung, und der Datenumfang ebenfalls klar definiert werden. Der noch unzureichende Entwurf kam in der 5. Legislaturperiode nicht über einen Referententext hinaus.

21.5 Projekt „Terminkalender für Schülerinnen und Schüler“

Im Auftrag des Landes sollte durch eine Hochschule in Zusammenarbeit mit einer Firma ein Terminkalender für Schülerinnen und Schüler der 7. bis 10. Klassen erstellt werden. Der Praxisnutzen des Hausaufgaben- und Terminplaners sollte mit einem umfassenden jugendgerechten Informationsangebot zu beruflichen Chancen und Perspektiven verbunden werden. Eine Identifikation der Schüler war nicht vorgesehen, es sollte lediglich ein Fantasiename benutzt werden und eine E-Mail-Adresse vorliegen, an die ggf. ein neues Kennwort gesandt werden könnte. Weiter war eine Evaluierung vorgesehen. Sie sollte detailliert sein, den Ort der Schule, die Schulform und die Klasse sowie das Geschlecht einbeziehen.

Aufgrund der engen Fristsetzung war eine differenzierte datenschutzrechtliche Bewertung des Vorhabens nicht möglich. Eine weitergehende datenschutzrechtliche Begleitung wurde angeboten. Vorab konnte aber auf Folgendes hingewiesen werden.

Zunächst wurde erläutert, dass die Hochschule als Betreiber des Terminkalenders Telemedienanbieter wird und das Telemediengesetz (TMG) beachten muss. Nach § 13 Abs. 4 TMG sind daher Daten über den Ablauf des Zugriffs und Nutzungsdaten nach Nutzungsende zu löschen, soweit sie nicht für eine Abrechnung benötigt werden. Weiter wurden die Einschränkungen der Speicherung der IP-Adresse erläutert. Auf deren Speicherung wurde dann verzichtet.

Ein wesentlicher Aspekt war weiter, dass von einer Anonymisierung im Sinne des § 2 Abs. 7 DSG-LSA nach den wenigen vorliegenden Informationen nicht ausgegangen werden konnte. Die Datenschutzerklärung der Hochschule sah unter „anonyme Daten“ die Fragen nach Klasse, Schule, Ort der Schule und Geschlecht vor. Der betroffene Personenkreis wird durch diese Informationen aber zumeist einerseits räumlich lokalisiert und andererseits auf eine Zahl

von unter 20 begrenzt. Hier wäre beispielsweise an kleine Gemeinden zu denken, die lediglich über eine Schule verfügen. Wird beispielsweise eine Schule in der in Frage kommenden Klassenstufe zufällig einzügig geführt, dürfte der Kreis der in Frage kommenden Personen räumlich identifiziert und auf unter 10 begrenzt sein.
Da ein Zusammenhang mit einem jugendgerechten Informationsangebot zu beruflichen Chancen und Perspektiven in Sachsen-Anhalt vorgesehen ist, stellte sich die Frage, ob und inwieweit diesbezügliche Angaben der Jugendlichen zu persönlichen Neigungen in das System aufgenommen werden können. Hierbei würde es sich um äußerst sensible Daten handeln. Demgemäß wurde empfohlen, zur Vermeidung eines Personenbezuges insoweit nachzuarbeiten.

Allgemein wurde angeraten deutlich zu machen, wer die für die Datenerhebung und Verarbeitung verantwortliche Stelle (§ 2 Abs. 8 DSG-LSA) ist. Soweit die Zusammenarbeit mit der Firma stattfindet, sollte geprüft werden, ob eine Datenverarbeitung im Auftrag vorliegt und ggf. wie diese ausgestaltet ist. Auf § 8 DSG-LSA wurde hingewiesen.

21.6 Datenübermittlungen von Schulen an Sportvereine

Durch mehrere Petenteneingaben wurde der Landesbeauftragte auf den Runderlass (RdErl.) des Kultusministeriums vom 16. Dezember 2008 zur Zusammenarbeit von Schulen und Sportvereinen bei der individuellen Förderung von Schülerinnen und Schülern aufmerksam gemacht.

Für die danach vorgesehenen Übermittlungen von personenbezogenen Daten von Schülern durch die Schule an Sportvereine lag keine gesetzliche Rechtsgrundlage vor, da die Übermittlungen nicht erforderlich im Sinne des § 84a Abs. 3 Satz 1 SchulG LSA bzw. des § 84a Abs. 2 SchulG LSA i. V. m. § 12 DSG-LSA waren. Der o. g. RdErl. sieht daher auch vor, dass eine Datenübermittlung nur dann zulässig ist, wenn der Betroffene eingewilligt hat. Hierfür soll das in der Anlage zum RdErl. beigefügte Formblatt verwendet werden.

Die Adressaten der Schülerdaten waren vielfältig (Landessportbund, einschließlich Stadt- und Kreissportbund, Landesfachverbände, Sportvereine). Zweck ist die Anerkennung sportlicher Leistungen, u. a. durch Vergabe des Sportabzeichens durch den Landessportbund und die individuelle Förderung des Betroffenen durch die jeweiligen weiteren Datenempfänger. Die Leistungen für das Sportabzeichen wurden zwar im Rahmen des Schulsports erbracht, die Anerkennung, d. h. das Abzeichen, war jedoch von der Einwilligung abhängig, die lediglich vollständig die Übermittlung teils sensibler Daten (Sportnoten und Werte aus motorischen Testverfahren) und deren weitere Verwendung vorsah.
Die Ausgestaltung des Verfahrens sicherte die Möglichkeiten der Sportförderung der Schüler, die Würdigung besonderer sportlicher Leistungen und die Förderung des Nachwuchsleistungssportes außerhalb der Schule.

Dem Landesbeauftragten schien jedoch, wie auch einigen besorgten Eltern, die Koppelung der Anerkennung der im Rahmen des Schulsports erbrachten Leistungen durch das Sportabzeichen mit der notwendigen Einwilligung auch

in die weitere Verwendung der Schülerdaten für einen nur grob umrissenen Adressatenkreis nicht unbedenklich. Gegebenenfalls würden Kinder an der Teilhabe an dem motivierenden Projekt des Sportabzeichens gehindert, wenn die Eltern die Weitergabe der Daten an Dritte außerhalb des Landessportbundes nicht befürworten. Die Freiwilligkeit der Einwilligung erschien daher ebenfalls zweifelhaft.

Leider stellte der gerade erst veröffentlichte RdErl. das Ergebnis aufwändiger Verhandlungen dar, sodass eine sofortige Änderung problematisch geworden wäre. Der Landesbeauftragte konnte aber dennoch in Beratungen eine datenschutzrechtliche Verbesserung erreichen. Das Kultusministerium erklärte sich erfreulicher Weise bereit – vorbehaltlich einer sicher grundsätzlich notwendigen Neufassung des Formblatts – den Schulen vorzugeben, die Eltern darauf hinzuweisen, dass die Einwilligung auf den Komplex des Sportabzeichens begrenzt und die weiteren Adressaten gestrichen werden dürfen. Auch der Landessportbund hat dies dankenswerter Weise akzeptiert.

22 Sozialwesen

22.1 Arbeitslosengeld II

Die im IX. Tätigkeitsbericht (Nr. 21.1) angekündigte Neuregelung ist erfolgt: Zum 1. Januar 2011 hat sich die Zuständigkeit bei der Datenschutzkontrolle im Bereich SGB II geändert. Seitdem ist grundsätzlich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Der Landesbeauftragte kontrolliert die Einhaltung des Datenschutzes nur noch bei den sogenannten Optionskommunen im Land, d. h. Einrichtungen in ausschließlich kommunaler Trägerschaft. Das sind zunächst die Landkreise Anhalt-Bitterfeld, Harz, Saalekreis und Salzlandkreis. Mit Inkrafttreten der Kommunalträger-Zulassungsverordnung am 1. Januar 2012 werden in Sachsen-Anhalt auch die Landkreise Altmarkkreis Salzwedel und Burgenlandkreis neben den o. g. Kreisen die Aufgaben nach dem SGB II in alleiniger Zuständigkeit wahrnehmen und somit der Kontrolle des Landesbeauftragten unterliegen. Leistungsberechtigte aus diesen Landkreisen können sich mit ihren Beschwerden nach wie vor an den Landesbeauftragten wenden, alle anderen an den Bundesbeauftragten.

22.2 Kontroll- und Beratungsbesuche bei Arbeitsgemeinschaften (ARGEn)

Auch im Berichtszeitraum hat der Landesbeauftragte bei den ARGEn vor Ort (die jetzt einheitlich Jobcenter heißen) in der Regel einzelfallunabhängige Beratungen und Kontrollen durchgeführt. In Zukunft werden sich die Kontrollen wegen der unter Nr. 22.1 geschilderten Zuständigkeitsänderung auf die Optionskommunen im Land beschränken müssen.

Grundsätzliche oder gravierende Mängel wurden während der Prüfungen nicht festgestellt. Auffällig war aber, dass von der Möglichkeit, Kopien anzufertigen, oft zu rege Gebrauch gemacht wird (z. B. Personalausweis, Mutterpass, Kontoauszüge). Ein besonders beliebter Vordruck scheint zudem die „Mietbescheinigung“ zu sein, die dem Hilfebedürftigen von mancher ARGE quasi regelmäßig mit der Bitte ausgehändigt wird, er möge die Angaben zu seiner Wohnung vom Vermieter bestätigen lassen, als ob nicht schon der

Mietvertrag generell alle erforderlichen Daten enthalten würde. Dies sieht der Landesbeauftragte sehr kritisch.
Die Verwendung der „Mietbescheinigung“ ist datenschutzrechtlich besonders bedenklich, wenn sie in jedem Einzelfall ohne konkrete Notwendigkeit erfolgt. Das führt dazu, dass von jeder Bedarfsgemeinschaft äußerst umfänglich personenbezogene Daten zur Wohnungssituation erhoben werden, die in einer Vielzahl von Fällen zur Feststellung der angemessenen tatsächlichen Aufwendungen für Unterkunft und Heizung nicht erforderlich sind. Dies ist unverhältnismäßig und ein Verstoß gegen das Gebot der Datenvermeidung und Datensparsamkeit (§§ 1 Abs. 2 Satz 1 DSG-LSA, 78 b SGB X). Außerdem wird auf diesem Weg dem Vermieter die Hilfebedürftigkeit seiner Mieter unbefugt offenbart und so gegen das Sozialgeheimnis verstoßen (§ 35 Abs. 1 Satz 1 SGB I).

22.3 Außendienst

Immer wieder bereitet der Einsatz von Außendiensten datenschutzrechtliche Probleme, insbesondere wenn es sich dabei um – vornehmlich unangekündigte – Hausbesuche beim Leistungsberechtigten zur Feststellung bzw. Überprüfung eines Bedarfs handelt. Dabei machen die mittlerweile mehrfach unter tatkräftiger Mithilfe der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten, von der Bundesagentur erlassenen „Fachlichen Hinweise zu § 6 SGB II“ viele hilfreiche Vorgaben – auch zum Datenschutz.

Problematisch bleibt, auch nach dem unter Nr. 22.1 geschilderten Zuständigkeitswechsel in der Datenschutzkontrolle, dass die Optionskommunen mit eigenen Regelungen oft zuungunsten der Hilfeempfänger von den Vorgaben der „Fachlichen Hinweise“ abweichen. Deshalb weist der Landesbeauftragte ausdrücklich darauf hin, dass Hausbesuche grundsätzlich angekündigt werden sollten und nur dann von einer Terminankündigung abzusehen ist, wenn konkrete Anhaltspunkte dafür vorliegen, dass ansonsten der Erfolg der Maßnahme gefährdet wäre.

Außerdem fehlt in den Regelungen der Optionskommunen häufig ein deutlicher Hinweis, dass vor der Einschaltung des Außendienstes die eigenen Möglichkeiten der Sachverhaltsaufklärung umfassend auszuschöpfen sind. Keinesfalls darf der Außendienst mit Sachverhaltsprüfungen beauftragt werden, die der Sachbearbeiter selber erledigen oder mit anderen Mitteln erreichen kann. Dies gebietet schon der Grundsatz der Verhältnismäßigkeit.

22.4 Vermittlungsvorschläge

Den Leistungsträgern der Grundsicherung für Arbeitssuchende obliegt nach § 4 Abs. 1 Nr. 1 SGB II die Unterstützung der Kunden mit dem Ziel der Eingliederung in Arbeit. Hierzu bedienen sie sich häufig des sogenannten Vermittlungsvorschlages. Dabei wird dem stellenanbietenden Arbeitgeber der Besuch des Kunden unter Verwendung von personenbezogenen Daten angekündigt. Allerdings wird dem Arbeitgeber bereits vor dem Bewerbungsgespräch die Situation des Bewerbers (arbeitslos, Sozialleistungsempfänger) offenbart. Daran hatte der Landesbeauftragte im Hinblick auf die Erforderlichkeit einer Übermittlung auf der Grundlage des § 69 Abs. 1 Nr. 1 SGB X in Prüfungen vor Ort Zweifel geäußert.

Teilweise erschien die Argumentation der Leistungsträger zumindest nachvollziehbar. Vermittlungsvorschläge erfolgen nur dann, wenn der Leistungsträger nach intensiver Prüfung davon ausgeht, dass das Anforderungsprofil der Stelle und das Kompetenzprofil des Kunden in Übereinstimmung zu bringen sind. Im Hinblick auf den Erfolgsdruck steht die Qualität der Vermittlungsvorschläge gegenüber der Quantität im Vordergrund.
Die Leistungsträger decken zudem nur einen kleinen Anteil des bundesweiten Vermittlungsbedarfs ab. Demgemäß können sie nur diejenigen Arbeitgeber in ihr Vermittlungsangebot aufnehmen, die wegen sachgerechter Vermittlungsvorschläge an einer weiteren Zusammenarbeit interessiert sind. Neben persönlichen Ansprechpartnern für die Kundenvermittlung wird daher auch Personal für die Betreuung der Arbeitgeber beschäftigt. Die Aufrechterhaltung und Betreuung eines Arbeitgeberbestandes sei zwingend erforderlich, um überhaupt dem Vermittlungsauftrag nachkommen zu können. Hier gelte es, in häufigen Kontakten zu überprüfen, ob und inwieweit das Vermittlungsangebot an die Arbeitgeberanforderungen angepasst werden kann.
Zudem sei es auch im Hinblick auf den Kunden regelmäßig erforderlich, mit dem Arbeitgeber in Verbindung zu treten. Zunächst müsse einmal zur Prüfung der Einhaltung von Mitwirkungspflichten und eventueller Sanktionsmöglichkeiten die tatsächliche Teilnahme an Bewerbungsterminen geklärt werden. Auch ist es für die Vermittler von Interesse zu erfahren, weshalb die für geeignet erachteten Bewerber sich letztendlich nicht haben durchsetzen können. Soweit hier Ursachen in der Person des Kunden (z. B. Auftreten) liegen, könnte der Leistungsträger zur Erfüllung des Vermittlungsauftrages gehalten sein, entsprechende qualifizierende Maßnahmen zu veranlassen.
Weiter war bei der Bewertung zu berücksichtigen, dass einem Großteil der Arbeitgeber bereits bekannt sein dürfte, dass die Bewerber aufgrund eines Vorschlags der Arbeitsgemeinschaft vorstellig werden. Ein großer Teil der Arbeitgeber, denen Vermittlungsvorschläge gesandt werden, erstellen Angebote nur gegenüber dem Leistungsträger.
Gelegentlich ist der Leistungsträger auch vorab inhaltlich unterstützend tätig. Dies kann beispielsweise erforderlich sein, um dem potentiellen Arbeitgeber den Kunden trotz des nicht ganz kompatiblen Leistungsprofils im Hinblick auf seine besondere Motivation nahe zu bringen.

Insgesamt konnte sich der Landesbeauftragte daher der Einschätzung nicht verschließen, dass in vielen Fällen die Sozialdatenübermittlung durch Vermittlungsvorschläge zur Aufgabenerfüllung der Leistungsträger erforderlich sein dürfte. Demgemäß wurde angeregt, jedenfalls in den Fällen, in denen absehbar ist, dass keine Weiterbearbeitung im o. g. Sinne erfolgt, dass auf die Versendung eines Vermittlungsvorschlages verzichtet wird.

22.5 Akteneinsicht im Verfahren nach SGB II

Eine Arbeitsgemeinschaft (ARGE), bei der auch sonst einiges im Argen lag, hatte einem Petenten zwar Einsicht in seine Akte gewährt, wollte aber selbst darüber bestimmen, welche Aktenbestandteile für den Leistungsempfänger von Interesse sein könnten. Das gefiel dem Petenten nicht so recht – zu Recht.

Gemäß § 25 Abs. 1 Satz 1 SGB X hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis

zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Dabei ist es in Rechtsprechung und Kommentarliteratur unstreitig, dass bei der Beurteilung, ob die Kenntnis bestimmter Akten bzw. Aktenteile erforderlich ist, nicht die Auffassung der Behörde maßgeblich sein kann. Es kann deshalb auch nicht auf die Auffassung der Behörde über die für die Entscheidung maßgeblichen Rechtssätze und die insoweit erheblichen Tatsachen ankommen. Wird zum Beispiel im Hinblick auf eine andere Rechtsauffassung des Beteiligten für einen beabsichtigten anderen Tatsachenvortrag oder für beabsichtigte Anträge und andere Ausführungen zu Sach- oder Rechtsfragen die Einsicht in Akten oder Aktenteile begehrt, die nach Auffassung der Behörde nicht maßgeblich sind, so ist diese Einsicht dennoch gem. § 25 SGB X dem Beteiligten zu gewähren. Wesentlicher Zweck der Akteneinsicht ist nämlich auch, den Beteiligten die Kenntnisse zu vermitteln, die sie für die sinnvolle und zweckentsprechende Ausübung Ihres Anspruchs auf rechtliches Gehör benötigen. Demnach sind von der Akteneinsicht nur solche Akten bzw. Aktenteile ausgeschlossen, die unter keinem denkbaren Gesichtspunkt für die Entscheidung von Bedeutung sein können. Im Zweifel hat die Behörde zugunsten einer Offenlegung zu entscheiden.

Soweit die Akteneinsicht zu gestatten ist, können die Beteiligten Auszüge oder Abschriften selbst fertigen oder sich Ablichtungen durch die Behörde erteilen lassen (§ 25 Abs. 5 Satz 1 SGB X).

Das sah schließlich auch die ARGE ein, sodass der Landesbeauftragte auf eine förmliche Beanstandung doch noch verzichten konnte.

22.6 Irrtümlich Mitglied einer Bedarfsgemeinschaft?

Irrtümlich zum Mitglied einer Bedarfsgemeinschaft gemacht sah sich ein selbständiger Petent, der sich beim Landesbeauftragten beschwerte und versicherte, zu keinem Zeitpunkt Leistungen bei der Arbeitsgemeinschaft (ARGE) beantragt oder bekommen zu haben. Wie sich herausstellte, war der Petent Eigentümer eines Hauses, in dem er mit der Leistungsberechtigten und drei gemeinsamen Kindern lebte. Deshalb war die ARGE auch befugt, vom Petenten personenbezogene Daten zu erheben und ihn, bis zum Beweis des Gegenteils, als Teil der Bedarfsgemeinschaft anzusehen.

Nach § 7 Abs. 3 Nr. 3 c) SGB II gehört nämlich zur Bedarfsgemeinschaft – neben dem erwerbsfähigen Hilfebedürftigen – auch eine Person, die mit dem erwerbsfähigen Hilfebedürftigen in einem gemeinsamen Haushalt so zusammenlebt, dass nach verständiger Würdigung der wechselseitige Wille anzunehmen ist, Verantwortung füreinander zu tragen und füreinander einzustehen. Gemäß § 7 Abs. 3a SGB II wird ein wechselseitiger Wille, Verantwortung füreinander zu tragen und füreinander einzustehen, vermutet, wenn Partner länger als ein Jahr zusammenleben, mit einem gemeinsamen Kind zusammenleben, Kinder oder Angehörige im Haushalt versorgen oder befugt sind, über Einkommen oder Vermögen des Anderen zu verfügen. Diese gesetzliche Vermutung konnte der Petent nicht widerlegen.

22.7 Kundenportal

Viel Mühe hatte sich ein Petent gemacht, der seiner Eingabe sogar ein Foto mit Anmerkungen beifügte, um seinem Unbehagen darüber Ausdruck zu verleihen, dass in einem Jobcenter bzw. einer Arbeitsagentur Kundengespräche im Wartebereich stattfinden müssten.

Ganz so tragisch war der Sachverhalt dann doch nicht, wie sich aus den Stellungnahmen der zuständigen Behörden ergab: „Die Bundesagentur für Arbeit hat mit ihrer neuen Organisationsstruktur den Empfang und die Eingangszone als Teil des Kundenportals bewusst offen gestaltet. Das bedeutet, die Arbeitsplätze sind für die Kunden einsehbar und direkt zugänglich. Für Kunden, die einen besonderen Schutz der Vertraulichkeit wünschen, stehen abgeschlossene Dienstzimmer (Diskretionszimmer) zur Verfügung. Sowohl am Empfang als auch im Wartebereich der Eingangszone sind entsprechende Hinweisschilder angebracht. Hier werden die Kunden darauf hingewiesen, dass sie nach der Anmeldung am Empfang von einem Mitarbeiter aus der Eingangszone aufgerufen werden. Auf den Arbeitsplätzen der Mitarbeiter stehen zusätzlich Hinweisschilder für den Fall, dass der Kunde aus datenschutzrechtlichen Gründen sein Anliegen in einem separaten Büro besprechen möchte."

Der Landebeauftragte sah den Schutz des Sozialgeheimnisses, bezogen auf seinen Zuständigkeitsbereich, noch als gewahrt an, weil die Betroffenen selbst über die von ihnen gewünschte Verfahrensweise bestimmen können.

22.8 Aufruf im Wartezimmer

Ein Petent hatte sich schon länger mit der Frage des namentlichen Aufrufs in Warteräumen, z. B. bei Ärzten oder der Arbeitsgemeinschaft, beschäftigt. Andere Kunden, die den Petenten ggf. vom Sehen her kennen, könnten so nun auch den Namen erfahren. Dies erschien dem Petenten datenschutzrechtlich bedenklich. Für den Bereich der öffentlichen Stellen konnten die Bedenken im Wesentlichen bestätigt werden.

Grundsätzlich bedarf die Übermittlung von personenbezogenen Daten an Dritte einer Rechtsgrundlage (§ 4 Abs. 1 DSG-LSA). Das persönliche Erscheinen im Warteraum eines Amtes mit der Gefahr, durch Bekannte erkannt zu werden, geschieht durch eigene, zumeist freiwillige Veranlassung und erscheint sozialadäquat.

Die durch behördlichen Aufruf ergehende Mitteilung an Mithörende, aus der sich ergibt, dass Betroffene, namentlich benannt, beispielsweise mit einem Sozialleistungsträger in Verbindung stehen, kann eine entsprechende Übermittlung darstellen. Solange für derartige Übermittlungen keine spezifischen Rechtsvorschriften vorliegen, sind die Übermittlungsregelungen des DSG-LSA bzw. bei Sozialdaten die des SGB X anzuwenden. An der danach notwendigen Erforderlichkeit dürfte es jedoch zumeist mangeln. Der Aufruf ist in der Regel mit anderen Methoden (z. B. "Der Nächste bitte.", Verwendung von Wartemarken) ohne Nennung von Namen und damit des Eingriffs in das Persönlichkeitsrecht möglich. Insbesondere im Sozialleistungsbereich begründet das Sozialgeheimnis die Pflicht des Leistungsträgers, das Sozialge-

heimnis (§ 35 SGB I) zu wahren. Die öffentlichen Stellen sind grundsätzlich durch § 6 DSG-LSA bzw. § 78a SGB X verpflichtet, durch technisch-organisatorische Maßnahmen sicherzustellen, dass nicht unbefugt personenbezogene Daten übermittelt werden. Ob die öffentliche Stelle eventuell von einer konkludenten Einwilligung ausgehen kann, hängt von den Umständen des Einzelfalls ab und erscheint eher fraglich. Die widerspruchslose Hinnahme von "herkömmlichen" Aufrufmethoden besagt nicht, dass der Betroffene dieses Verfahren konsentiert. Zudem bestünde in der Regel die Möglichkeit, die Betroffenen zu befragen. Namentliche Aufrufe sind daher grundsätzlich zu vermeiden.

22.9 Löschung der Telefonnummer

Ein Petent hatte sich im vorherigen Berichtszeitraum (vgl. IX. Tätigkeitsbericht, Nr. 21.5) beschwert, dass ein Leistungsträger seine freiwillig angegebene Telefonnummer nicht entsprechend § 84 Abs. 2 SGB X wieder löschen wollte. Der Leistungsträger hatte die Auffassung vertreten, dass die Speicherung der Telefonnummer für die Erfüllung der Aufgaben nach dem SGB II, insbesondere für die Eingliederung in Arbeit, erforderlich sei. Doch der Landesbeauftragte hatte ihn schließlich davon überzeugen können, dass dem nicht so ist. Ein Anruf kann zwar oft hilfreich sein, die Vermittlung ist aber auch möglich, wenn der Betroffene kein Telefon hat.

Groß war deshalb die Überraschung, als sich der gleiche Petent erneut an den Landesbeauftragten wandte, weil er wieder von dem Leistungsträger angerufen worden war. Wie sich herausstellte, war er es selbst, der gegenüber einem Maßnahmeträger doch wieder seine Telefonnummer angegeben hatte, die so in die Akte des Leistungsträgers „gewandert“ war. Inzwischen sollen alle Telefonnummern des Petenten in der Akte geschwärzt worden sein.

Durch eine weitere Eingabe zu diesem Thema ist dem Landesbeauftragten deutlich geworden, dass es noch immer Leistungsträger geben muss, die Vordrucke verwenden, in denen die Telefonnummer nicht als freiwillige Angabe gekennzeichnet ist. Er hofft, dass es damit bald ein Ende hat.

22.10 Elektronischer Entgeltnachweis (ELENA)

Seit Anfang 2010 sind die Arbeitgeber gesetzlich verpflichtet, die monatlichen Gehaltsdaten ihrer Beschäftigten wie Name und Anschrift, Versicherungsnummer, Bruttoeinkünfte und Abzüge für die Sozialversicherung an die Zentrale Speicherstelle (ZSS), die bei der Deutschen Rentenversicherung Bund angesiedelt ist, zu übermitteln. Die Behörden sollten diese Daten ab 2012 bei der Bearbeitung von Anträgen auf staatliche Leistungen (z. B. Arbeitslosen-, Wohn- oder Elterngeld) verwenden. Weitere Sozialleistungen sollten im späteren Verfahrenslauf hinzukommen. Aufgrund komplexer technischer Fragen ist eine termingerechte Umsetzung in den beteiligten Behörden jedoch fraglich. Ein Verschieben des Abrufstarts auf den Januar 2014 wurde diskutiert.

Darüber hinaus haben über 20.000 Personen verfassungsrechtliche Bedenken gegen ELENA mit einer Sammelverfassungsbeschwerde geltend gemacht. Die Bedenken beziehen sich hauptsächlich auf die Frage unzulässiger Vorratsdatenspeicherung. Landesbeauftragte für den Datenschutz der

Länder haben hierzu eine Stellungnahme gegenüber dem Bundesverfassungsgericht abgegeben. Darin wird auf einzelne verfassungsrechtliche Problemlagen hingewiesen.

Der Bundesbeauftragte und einzelne Landesbeauftragte waren in Arbeitskreisen vertreten, die sich u. a. mit Verfahrensfragen zu ELENA befassen. Auf diese Weise konnte beispielsweise die Erhebung und Speicherung von Fehlzeiten aufgrund von Arbeitskämpfen in der zentralen Datenbank verhindert werden.

Darüber hinaus war festzustellen, dass das Auskunftsrecht nach § 103 Abs. 4 SGB IV derzeit noch nicht zu verwirklichen war; die entsprechenden technischen Voraussetzungen fehlten.

Am 18. Juli 2011 teilten die zuständigen Bundesministerien mit, dass ELENA schnellstmöglich eingestellt werde. Grund sei die ungenügende Verbreitung der qualifizierten elektronischen Signatur und somit ein datenschutzrechtliches Defizit bei der Datenübermittlung. Hintergrund ist wohl auch die Belastung der Unternehmen. Die bereits gespeicherten Daten sollen unverzüglich gelöscht werden – dafür bedarf es noch einer gesetzlichen Anordnung.

22.11 Abrechnung bei der hausarztzentrierten Versorgung

Nach § 73b Abs. 1 SGB V haben die Krankenkassen ihren Versicherten eine besondere hausärztliche Versorgung (hausarztzentrierte Versorgung) anzubieten. Auch die im Rahmen der hausarztzentrierten Versorgung erbrachten ärztlichen Leistungen sind gemäß § 295 Abs. 4 SGB V grundsätzlich über die Kassenärztlichen Vereinigungen mit den Krankenkassen abzurechnen. § 295 Abs. 1b Satz 5 SGB V erlaubt aber ebenso die Beauftragung einer „anderen Stelle“. Diese nachträglich eingefügte und nur befristet gültige (allerdings immer wieder verlängerte) Vorschrift ist die unmittelbare Reaktion des Gesetzgebers auf ein Urteil des Bundessozialgerichts in einem ähnlichen Sachverhalt, wonach Krankenhäuser sowie Vertragsärzte Patientendaten, die gesetzlich Krankenversicherte betreffen, nicht zur Erstellung der Leistungsabrechnung an private Dienstleistungsunternehmen übermitteln dürfen (IX. Tätigkeitsbericht, Nr. 21.13).

Im Berichtszeitraum ist es deswegen in einigen Bundesländern zu datenschutzrechtlichen Problemen bei der Abrechnung der hausarztzentrierten Versorgung gekommen. Nicht so bei der AOK Sachsen-Anhalt, wo die Abrechnung über die Kassenärztliche Vereinigung erfolgt. Aber in Schleswig-Holstein hat das dortige Unabhängige Landeszentrum für Datenschutz in einer Verfügung dem Hausärzteverband Schleswig-Holstein e.V. (HÄV SH) unter Androhung eines Zwangsgeldes in Höhe von 30.000 Euro untersagt, gemäß dem zwischen der AOK Schleswig-Holstein, dem HÄV SH und Dienstleistern abgeschlossenen Vertrag von eingeschriebenen Hausärzten stammende Patientendaten weiterzugeben oder diese selbst zu nutzen. Damit sind die in dem HÄV SH zusammengeschlossenen Hausärztinnen und Hausärzte nicht berechtigt, Abrechnungsdaten auf dem im Vertrag vorgesehenen elektronischen Weg zu übermitteln. Grund dieser Anordnung ist, dass die Hausärzte faktisch keine ausreichende Möglichkeit der Kontrolle über die Weitergabe von Patientendaten durch ihr Praxissystem mehr hätten. Der

Vertrag sieht vor, dass sich die Ärzte des HÄV SH als Auftragsdatenverarbeiter bedienen müssen, wenn sie von den für sie günstigen Hausarztabrechnungen Gebrauch machen wollen. Tatsächlich sind sie aber weder rechtlich noch faktisch in der Lage, die Kontrolle über ihre Patientendaten als Auftraggeber wahrzunehmen. An dem Rahmenvertrag, der das Verhältnis zwischen dem HÄV SH, Dienstleistern und den einzelnen Ärzten festlegt, sind letztere überhaupt nicht beteiligt. Darin werden diese gezwungen, auf ihren Praxissystemen Software gemäß den Vorgaben des Hausärzteverbandes zu installieren, womit das Auftragsverhältnis geradezu auf den Kopf gestellt wird. Ihnen wird sogar vertraglich verboten, Kenntnis von wesentlichen Elementen der Software zu nehmen, sodass sie faktisch keine vollständige Kontrolle mehr über die Daten auf ihrem System hätten. Damit würden sie nicht nur ihre Datenschutzpflichten verletzen, sondern auch ihre ärztliche Schweigepflicht. Ähnliche Problemlagen und datenschutzrechtliche Bedenken gibt es auch in anderen Bundesländern. In Schleswig-Holstein wurde die o. g. Untersagung des Unabhängigen Landeszentrums für Datenschutz im einstweiligen Rechtsschutzverfahren vor dem Oberverwaltungsgericht im Januar 2011 bestätigt (Beschluss vom 12. Januar 2011, 4 MD 56/10).

In diesem Zusammenhang sah sich die 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2010 veranlasst, in einer Entschließung „klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung“ zu verlangen (**Anlage 11**).

Am 28. Juli 2011 wurde mit dem „Gesetz zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze“ ein neuer § 295a SGB V eingefügt (BGBl. I S. 1622). Der § 295a SGB V regelt nunmehr die Einbeziehung von Vertragspartnern auf Leistungserbringerseite in die Abrechnung. Für sie und ihre Auftragnehmer gilt § 35 SGB I entsprechend. Voraussetzung ist, dass der Versicherte neben der Teilnahmeerklärung an der Versorgungsform die Einwilligung in die damit verbundene Datenübermittlung erklärt. Gewisse datenschutzrechtliche Bedenken bleiben trotz der differenzierten Regelung bestehen, denn damit liegen dann sensible Patientendaten nicht mehr bei öffentlichen Stellen im Sinne des § 35 SGB I mit der entsprechend strukturierten Aufsicht. Die betroffenen Daten sind unklar beschrieben. Auch die geforderte gesonderte Einwilligung in die Datenübermittlung trägt nur, wenn die notwendige Freiwilligkeit (Alternativen) gegeben ist.

22.12 Protokollierung bei IT-Verfahren in der Krankenversicherung

Änderungen der rechtlichen Rahmenbedingungen, die Erweiterung funktionaler Anforderungen, Zusammenschlüsse von Krankenkassen sowie die technische Entwicklung haben in der gesetzlichen Krankenversicherung zur grundlegenden Überarbeitung bzw. Neuentwicklung der eingesetzten IT-Verfahren geführt.

Angesichts der Komplexität derartiger Großverfahren mit ihrer hohen Zahl von Benutzern und Transaktionen, verteilten IT-Strukturen und Verantwortlichkeiten bedarf es für eine datenschutzgerechte Gestaltung auch eines geeigneten Instrumentariums, um die Verarbeitung personenbezogener Daten nachvollziehen zu können. Grundlage einer angemessenen Nachvollziehbar-

keit ist eine aussagefähige Protokollierung einschließlich geeigneter Auswertungsmöglichkeiten.

Die Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben deshalb mit Stand vom 19. März 2010 „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der gesetzlichen Krankenversicherung“ veröffentlicht; das Papier steht auf der Homepage des Landesbeauftragten zur Verfügung. Die Empfehlungen sollen auch auf diesem Wege einer interessierten Öffentlichkeit zur Kenntnis gegeben werden. Der Landesbeauftragte hofft, dass sie bei allen IT-Verfahren in der gesetzlichen Krankenversicherung berücksichtigt werden.

22.13 Betreuungsbehördendaten für die Berufsgenossenschaft

Die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) fragte beim Landesbeauftragten an, ob es datenschutzrechtlich möglich sei, Adressen von Berufsbetreuern von den Betreuungsbehörden übermittelt zu bekommen. Dies schien erforderlich, da eine große Zahl von beitragspflichtigen Berufsbetreuern vermutet wurde, die keinen Kontakt zur BGW aufgenommen hatten.
Die Übermittlung von personenbezogenen Daten durch eine öffentliche Stelle bedarf einer Rechtsgrundlage in Form einer Rechtsvorschrift oder der Einwilligung der jeweils Betroffenen (§ 4 Abs. 1 DSG-LSA). Im Betreuungsbehördengesetz (BtBG) fand sich keine entsprechende Regelung. Vielmehr ist in den §§ 4 ff. BtBG lediglich der Aufgabenkanon der Betreuungsbehörde beschrieben. Auch die Regelungen des Zweiten Kapitels des SGB X waren nicht einschlägig. Sie beziehen sich auf Sozialdaten, die von Stellen im Sinne des § 35 SGB I erhoben werden (§ 67 Abs. 1 SGB X). Die Betreuungsbehörden sind nicht erfasst.

Demgemäß kamen die Regelungen des DSG-LSA für die Landkreise als Betreuungsbehörden im Land Sachsen-Anhalt als mögliche Rechtsgrundlage in Betracht.
Nach § 11 Abs. 1 DSG-LSA ist die Übermittlung von personenbezogenen Daten an eine öffentliche Stelle, und damit an die Berufsgenossenschaft, zulässig, wenn die Übermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder der in der Zuständigkeit der Empfänger liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 10 DSG-LSA zulassen würden.

Die Aufgaben der Betreuungsbehörde sind in den § 4 ff. BtBG beschrieben und umfassen im Wesentlichen die Beratung, die Fortbildung und die Unterstützung der Tätigkeit von betreuenden Personen oder Organisationen. Unter diesen Aufgabenkanon war die Weiterleitung der Adressdaten der bekannten Berufsbetreuer zu Zwecken der Prüfung der Mitgliedschaft durch Berufsgenossenschaften nicht zu subsumieren.

Die Datenerhebung gehörte aber zum Aufgabenkreis der BGW, Erhebungsgrundlage ist § 199 Abs. 1 Satz 1 SGB VII i. V. m. § 67a Abs. 1 SGB X. Auch gegen eine Erhebung bei Dritten bestanden keine grundsätzlichen Bedenken (§ 67a Abs. 2 Satz 2 Nr. 2 b) bb) SGB X).

Nach § 10 DSG-LSA wäre die Nutzung und damit eine zweckändernde Übermittlung zulässig, wenn eine der Voraussetzungen des Absatzes 2 erfüllt ist. Nach § 10 Abs. 2 Nr. 3 DSG-LSA ist die Zweckänderung möglich, soweit offensichtlich ist, dass sie im Interesse des Betroffenen liegt und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde.

Zunächst konnte man davon ausgehen, dass die Verwendung der Adressinformationen durch die Betreuungsbehörde im Interesse des Betroffenen liegt, da sie der Feststellung des Versicherungsverhältnisses dient. Trotz der eventuellen Folge der Beitragszahlungspflicht ist aufgrund der gesetzlichen Vorgaben von einem objektiven Vorteil auszugehen. Fraglich erschien aber, ob Grund zu der Annahme besteht, dass der Betroffene in Kenntnis des neuen Zwecks seine Einwilligung verweigern würde. Hierfür könnte sprechen, dass einige der betroffenen Berufsbetreuer sich möglicherweise bewusst und gewollt gegen die Erfüllung der Mitteilungs- und Auskunftspflicht nach § 192 Abs. 1 SGB VII entschieden haben und diese Entscheidung unterlaufen werden könnte. Die Einschränkung in § 10 Abs. 2 Nr. 3 DSG-LSA ist Ausdruck des Selbstbestimmungsprinzips. Eine Freiheit zur Selbstbestimmung schien aber für den Fall nicht gegeben, dass der Betroffene uneingeschränkt zur Angabe von Name und Anschrift gesetzlich verpflichtet ist. Zudem liegt einer der klassischen Anwendungsfälle des § 10 Abs. 2 Nr. 3 DSG-LSA vor, wonach eine Verwendung der Daten zulässig ist, wenn der Betroffene nur unter sehr erschwerten Bedingungen bzw. gar nicht um eine persönliche Entscheidung gebeten werden kann, da er nicht erreichbar ist.

Ergänzend wurde gebeten, den Aspekt der Erforderlichkeit zu prüfen. Als Alternative war das Adressmittlungsverfahren zu prüfen. Es hätten den Betreuungsbehörden Schreiben an die Berufsbetreuer zur Weiterleitung zur Verfügung gestellt werden können, die die Berufsbetreuer an die Meldepflicht erinnern.

22.14 Kinderschutz

Wie bereits im IX. Tätigkeitsbericht (Nr. 21.16) dargestellt, wurde aufgrund verfassungsrechtlicher Bedenken der Teil des ursprünglichen Gesetzentwurfes zur Verbesserung des Schutzes von Kindern und zur Förderung der frühkindlichen Bildung (LT-Drs. 5/1331), der u. a. das verbindliche Einladungswesen für Früherkennungsuntersuchungen vorsah, herausgelöst.

Im Ergebnis war zur Sicherung des Kindeswohls ein Zentrum „Frühe Hilfen für Familien“ vorgesehen. Dieses Zentrum soll u. a. die lokalen Netzwerke Kinderschutz unterstützen, die Träger der öffentlichen und freien Jugendhilfe beraten, den landesweiten Erfahrungsaustausch organisieren und Handlungsempfehlungen geben.

Das Gesetz zur Verbesserung des Schutzes von Kindern ist am 22. Dezember 2009 in Kraft getreten (GVBl. LSA S. 644).

Als Auftaktveranstaltung fand im Juni 2010 eine Landeskonferenz zum Aufbau der Netzwerkarbeit statt. Um datenschutzrechtlichen Unsicherheiten von Beteiligten in lokalen Netzwerken zu begegnen, will das Zentrum für Frühe

Hilfen für Familien in Zusammenarbeit mit dem Landesjugendamt und dem Landesbeauftragten eine Handreichung über die datenschutzrechtlichen Befugnisse der einzelnen Akteure erarbeiten.

Darüber hinaus konnte der Landesbeauftragte bei der Aktualisierung des Leitfadens „Gewalt gegen Kinder und Jugendliche“ für Lehrerinnen und Lehrer und Erzieherinnen und Erzieher mitwirken.

Auch auf Bundesebene wurde eine Änderung beschlossen. Aufgrund des Gesetzes zur Änderung des Vormundschafts- und Betreuungsrechts soll der persönliche Kontakt zwischen Betreuern und Betreuten u. a. aufgrund der Verringerung der Fallzahlen auf 50 Vormundschaften je Mitarbeiter verbessert werden (BGBl. I 2011 S. 1306).

Darüber hinaus hat das Bundeskabinett den neuen Entwurf eines Bundeskinderschutzgesetzes beschlossen (IX. Tätigkeitsbericht, Nr. 21.15). Es sieht u. a. die Stärkung von Familienhebammen, ein erweitertes Führungszeugnis für hauptamtliche Mitarbeiter der Jugendhilfe und eine Befugnisnorm für Berufsgeheimnisträger hinsichtlich der Weitergabe von Informationen an das Jugendamt vor. Das Gesetz soll 2012 in Kraft treten (BR-Drs. 202/11).

22.15 Sprachstandsfeststellung und Sprachförderung

Zum 1. Januar 2009 trat das Gesetz zur Förderung der frühkindlichen Bildung in Kraft (GVBl. LSA 2008 S. 448). Damit wurde u. a. die verpflichtende Teilnahme an der Sprachstandsfeststellung im vorletzten Jahr vor der Einschulung eingeführt (IX. Tätigkeitsbericht, Nr. 21.16). Durch Verordnung waren nun das nähere Verfahren, die Zuständigkeiten usw. zu regeln.

Der Landesbeauftragte wurde bei der Erarbeitung der Verordnung zur Umsetzung der Sprachstandsfeststellung und Sprachförderung frühzeitig und umfassend beteiligt. Der Landesbeauftragte konnte u. a. erreichen, dass der Datenabgleich durch den Schulträger konkret geregelt wurde (Datenerhebungs- und -verarbeitungsbefugnisse, Festlegung eines Datensatzes, Datenlöschung). Hierfür ist eine Übermittlung von Meldedaten und von Daten aus den Kinderbetreuungseinrichtungen vorgesehen. Eine gesetzliche Übermittlungsbefugnis für die Kindereinrichtungen ist jedoch nicht gegeben (§ 64 Abs. 2 SGB VIII i. V. m. § 69 Abs. 1 SGB X), sodass eine Datenübermittlung an den Schulträger ausschließlich auf Basis der Einwilligung erfolgen kann. Auch wurde festgelegt, dass die in dem Verfahren erhobenen personenbezogenen Daten von den Kindertagesstätten zu löschen sind, sobald sie nicht mehr erforderlich sind, spätestens jedoch mit Beginn des Schuljahres, in dem das Kind in die Schule eintritt.

22.16 Elternbuch des Jugendamtes

Ein Jugendamt plante zur Erfüllung der Aufgaben nach § 16 Abs. 1 und Abs. 2 SGB VIII und § 52a Abs. 1 SGB VIII, allen Eltern eines neugeborenen Kindes, die es wünschen, anlässlich eines persönlichen Besuches durch Jugendamtsmitarbeiter ein Elternbuch zu überreichen. Dieses Angebot diene als Geste der Wertschätzung, der Möglichkeit des Kontakts im häuslichen Umfeld und zu allgemeinen und individuellen Beratungs- und Unterstüt-

zungsleistungen. Die Aufgaben des Jugendamtes könnten erläutert und Vorbehalte gegen die spätere Inanspruchnahme von Hilfen abgebaut werden. Die Adressen kämen von der Meldebehörde. Als Nebeneffekt wurde ein Beitrag zum effektiven Kinderschutz gesehen.

Aus datenschutzrechtlicher Sicht war u. a. auf Folgendes hinzuweisen:

Die Geburt eines Kindes, dessen Eltern nicht miteinander verheiratet sind, wird dem Jugendamt angezeigt. Nach § 52a Abs. 1 SGB VIII hat das Jugendamt der Mutter unverzüglich nach der Geburt des Kindes Beratung und Unterstützung anzubieten. Auch insoweit wären Hausbesuche aber nur auf einer Rechtsgrundlage möglich. Hierbei ist zu berücksichtigen, dass nicht nur das Grundrecht auf informationelle Selbstbestimmung, sondern auch das Wohnungsgrundrecht aus Art. 13 GG tangiert wäre. Der Einfluss auf die Freiwilligkeit einer Einwilligung durch die vorgesehene Koppelung der Überreichung des Elternbuchs und des Hausbesuchs wäre bedenklich. Das Verfahren stünde auch einer sinnvollen größeren Verbreitung des Elternbuchs entgegen.

Übermittlungen von personenbezogenen Daten von Kindern, deren Eltern miteinander verheiratet sind, von der Meldebehörde an das Jugendamt beurteilen sich nach § 29 Abs. 1 MG LSA i. V. m. § 11 Abs. 1 Nr. 1 DSG-LSA. Danach könnte die Anforderung der Adressen aller Neugeborenen/Eltern zulässig sein, soweit dies nach den §§ 61 ff. SGB VIII i. V. m. §§ 67 ff. SGB X zur Erfüllung der jeweiligen Aufgabe des Jugendamtes erforderlich ist (§ 62 Abs. 1 SGB VIII).

Gegen eine reine Begrüßung als Geste der Wertschätzung durch den Landrat bestehen keine grundsätzlichen Bedenken. Dies wäre aber eher Aufgabe des Landratsbüros. Die Tätigkeit des Jugendamtes in Erfüllung von Aufgaben der Jugendhilfe ist davon zu unterscheiden.

Die Formulierung der „jeweiligen Aufgabe“ stellt zudem klar, dass eine Datenerhebung einzelfallbezogen sein muss. Dementsprechend findet sich auch in den §§ 11 bis 60 SGB VIII keine Aufgabe, die generelle Ermittlungen des Jugendamtes ohne Anhaltspunkte im Einzelfall erfordert. Für eine regelmäßige und pauschale Datenerhebung bezüglich aller Eltern und deren neugeborenen Kindern im Hinblick auf den Schutzauftrag des Kindeswohls bietet § 62 Abs. 1 SGB VIII keine Rechtsgrundlage.

Nach § 8a SGB VIII ist die Wahrnehmung des Wächteramtes des Staates an konkrete und nicht unerhebliche Voraussetzungen gebunden. Die Nutzung von Begrüßungsbesuchen, um „bei Gelegenheit“ bzw. „als Nebeneffekt“ Tatsachen im Hinblick auf die Gefährdung des Kindeswohls zu erforschen, wäre wohl eine Umgehung der gesetzlichen Regelung. Allein die Tatsache einer Geburt begründet noch keine Befugnis der Jugendhilfe, ohne Einverständnis der Betroffenen tätig zu werden. Begrüßungsbesuche, die gezielt dazu genutzt werden, Tatsachen im Hinblick auf mögliche Kindeswohlgefährdungen allein deswegen zu ermitteln, weil ein Kind geboren wurde, können auch nicht auf § 8a SGB VIII gestützt werden.

Auch im Hinblick auf die Aufgabenstellung nach § 16 Abs. 1 SGB VIII bestanden gewisse Bedenken. Zwar sind allgemein Hilfen zur Erfüllung der allgemeinen Förderung der Erziehung in der Familie (§ 16 SGB VIII) anzubieten. Danach besteht die grundsätzliche Pflicht zur Förderung der Stärkung der familialen Erziehungskraft. Auch diese Angebote sind anlassunabhängig bzw. präventiv. Die meisten hierzu genannten Beispiele sehen jedoch keinen Umgang mit personenbezogenen Daten der Nutzer der Angebote vor, da nur Träger gefördert werden (Familienberatung, Familienerholung, Ehevorbereitungskurse usw.). Im Rahmen der Familienbildung kommt allerdings auch die Versendung von Elternbriefen in Betracht.

Die sachdienliche Aufklärung der Eltern von Neugeborenen über bestehende Hilfsangebote u. ä. durch mildere Mittel war daher zu prüfen. Dabei war auch das sog. Adressmittlungsverfahren zu erwägen, bei dem das Jugendamt den Meldebehörden vorbereitete Schreiben an die Betroffenen (Elternbrief) zur Verfügung stellt, die dann von den Meldebehörden unter Nutzung der bei ihnen vorhandenen Daten versandt werden.

Die Form der beabsichtigten Hilfen sollte in einem Anschreiben an die Eltern transparent gemacht werden. Der Hausbesuch als stärkstes Eingriffsmittel bedarf in der Regel entsprechender Anlässe. Hierfür würde eine möglicherweise wirksame Einwilligungserklärung der Betroffenen zumindest voraussetzen, dass sie über die Freiwilligkeit der Besuche, die Identität der verantwortlichen Stelle und über die verfolgten Zwecke hinreichend aufgeklärt wurden. Maßgeblich ist der veranlassende Wille der Eltern in Kenntnis aller möglichen Konsequenzen.

22.17 Wohn- und Teilhabegesetz

Seit Inkrafttreten der Föderalismusreform I zum 1. September 2006 ist die Gesetzgebungskompetenz für das Heimrecht auf die Länder übergegangen. Das Land Sachsen-Anhalt hat davon Gebrauch gemacht und das Wohn- und Teilhabegesetz erlassen (GVBl. LSA 2011 S. 136).

Der Landesbeauftragte wurde bereits sehr frühzeitig beteiligt. Seine Hinweise fanden Eingang in den Gesetzentwurf.

So wurde beispielsweise ausdrücklich geregelt, dass die im Internet zu veröffentlichenden Qualitätsberichte mit Ausnahme der Namen und Anschriften des Trägers und der Leitung keine personenbezogenen Daten enthalten. Darüber hinaus wurde ergänzt, dass hinsichtlich der technisch-organisatorischen Maßnahmen zum Datenschutz die Regelungen des DSG-LSA gelten.

Außerdem wurde für die Einrichtungsträger die Löschung von Aufzeichnungen über den Betrieb von stationären Einrichtungen nach fünf Jahren angeordnet.

22.18 Bundeselterngeld- und Elternzeitgesetz

Zum 1. Januar 2010 sind die Aufgaben nach dem Bundeselterngeld- und Elternzeitgesetz auf die Landkreise und kreisfreien Städte übergegangen.

Im Rahmen des Erfahrungsaustausches mit den behördlichen Datenschutzbeauftragten der Landkreise und kreisfreien Städte wurde an den Landesbeauftragten herangetragen, dass das vorgegebene Verfahren datenschutzrechtlichen Bedenken begegnen würde.

Anhand des vom Landesverwaltungsamt vorgelegten Verfahrensverzeichnisses hat der Landesbeauftragte das neue Verfahren einer datenschutzrechtlichen Prüfung unterzogen. Problematisch erschien der Zugriff auf personenbezogene Daten der Antragsteller durch Mitarbeiter des Landesverwaltungsamts und die nicht verschlüsselte Datenübermittlung von den Elterngeldstellen an das Landesrechenzentrum. Die Erforderlichkeit der Zugriffsberechtigung auf personenbezogene Daten konnte das Landesverwaltungsamt schlüssig begründen, da z. B. alle Widersprüche, die sich gegen Bescheide richten, die bis zum 31. Dezember 2009 durch die Elterngeldstellen des Landesverwaltungsamts erteilt wurden, dort bearbeitet werden.

Eine verschlüsselte Datenübertragung von allen Elterngeldstellen an das Landesrechenzentrum erfolgt nunmehr seit November 2010.

22.19 Elternadressen

Bei Anträgen auf Ausbildungsförderung in einem Landkreis waren einige Jugendliche nicht in der Lage, die Unterlagen zu Einkommensangaben der Eltern beizubringen, da sie nicht wussten, wo ihre Eltern wohnen. Das zuständige Amt für Ausbildungsförderung musste somit bei der Erstantragsstellung deren Adresse ermitteln und die Eltern zur Einkommenserklärung auffordern. Da die Adressermittlung und die folgende Anfrage bei den Eltern zu Mehraufwand führte, stellte sich die Frage, ob das Amt den betroffenen Jugendlichen die einmal ermittelte Adresse übergeben könne, um ihnen die Möglichkeit zu geben, sich direkt an ihre Eltern zu wenden und die Unterlagen für Folgeanträge beizubringen.

Die Förderung nach dem Bundesausbildungsförderungsgesetz gehört nach § 68 Nr. 1 SGB I als besonderer Teil zum Sozialgesetzbuch. Demgemäß sind die datenschutzrechtlichen Bestimmungen der §§ 67 ff. SGB X zu beachten. Daher hat der Landesbeauftragte zunächst auf § 67a Abs. 2 Satz 1 SGB X verwiesen, wonach Sozialdaten grundsätzlich beim Betroffenen zu erheben sind. Dies sollte Berücksichtigung finden, auch wenn üblicherweise die Antragsteller die erforderlichen Erklärungen ihrer Eltern selbst beibringen. Zudem geht es faktisch lediglich um den Versuch, geringe Verwaltungsaufwendungen einzusparen, in der Hoffnung, die Jugendlichen würden nunmehr selbst die erforderlichen Erklärungen der Eltern beibringen. In den Fällen, in denen dies aus Nachlässigkeit der Jugendlichen bei dem Erstantrag nicht erfolgte, wäre daher bereits kein Erfolg zu erwarten. Darüber hinaus kann es besondere Gründe, wie beispielsweise schützenswerte Interessen der Eltern, geben, weshalb dem Jugendlichen die Adresse nicht bekannt ist. Insoweit könnte ein gebotener Schutz der Sozialdaten gegenüber dem geringen fiskalischen Interesse überwiegen. Die Erforderlichkeit der Datenübermittlung, die nach § 69 Abs. 1 Nr. 1 SGB X Voraussetzung der zulässigen Adressübermittlung wäre, erschien daher zweifelhaft.
Demgemäß hat der Landesbeauftragte angeraten, die Eltern jeweils im Rahmen des Erstantragsverfahrens zu befragen, ob sie mit der Weiterleitung

von Adressdaten einverstanden sind. Dann bestünden gegen die Weiterleitung aus datenschutzrechtlicher Sicht keine Bedenken.

23 Statistik

23.1 Zensus 2011

Anders als der ursprüngliche Reichszensus römischer Prägung, der eine Steuerschätzung der Bürger des Imperiums war, ist der moderne Zensus, wie er im Gewande des Zensus 2011 daherkommt, eine möglichst exakte Zählung. Über die verschiedenen Phasen der Vorbereitung dieses größten Statistikvorhabens seit der Volkszählung von 1987 hatte der Landesbeauftragte in seinem VIII. Tätigkeitsbericht (Nr. 21.1) und seinem IX. Tätigkeitsbericht (Nr. 22.1) bereits berichtet.
Der Zensus 2011 ist keine rein deutsche Angelegenheit. Aufgrund der Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen ist der Zensus 2011 in allen Mitgliedstaaten der EU durchzuführen. Die Staaten, und im föderalen Systems Deutschlands auch die Länder, regeln für ihren Hoheitsbereich lediglich die Details der Durchführung des Zensus.
Der Zensus dient

- der Feststellung der amtlichen Einwohnerzahl von Bund, Ländern und Gemeinden,

- der Gewinnung von Grunddaten für das Gesamtsystem der amtlichen Statistik sowie von Strukturdaten über die Bevölkerung als Datengrundlage insbesondere für politische Entscheidungen von Bund, Ländern und Kommunen auf den Gebieten Bevölkerung, Wirtschaft, Soziales, Wohnungswesen, Raumordnung, Verkehr, Umwelt und Arbeitsmarkt sowie

- der Erfüllung der Berichtspflichten nach der o. g. EG-Verordnung.

Im Übrigen ist der Zensus 2011, obgleich solches immer wieder behauptet wird, keine Registerzählung bzw. kein Registerzensus. Vielmehr werden auf der Grundlage verschiedener Register allein in Sachsen-Anhalt

- alle ca. 625.000 Wohngebäude- bzw. Wohnungseigentümer und

- ca. 240.000 Einwohner, das sind rund 10 %,

befragt. Außerdem erfolgt direkt vor Ort die Erhebung von Daten über die Bewohner von Gemeinschaftsunterkünften und die Insassen der Justizvollzugsanstalten.

Für die Durchführung statistischer Erhebungen wie dem Zensus 2011 ist es von besonderer Bedeutung, den Kreis der zu Befragenden und deren statistische Zuordnung vorab möglichst genau zu kennen. Diesen Informationsbedarf wollten die Statistischen Ämter der Länder, also auch das Statistische Landesamt Sachsen-Anhalt, durch eine dem eigentlichen Zensus 2011 vorgeschaltete Erhebung im Oktober 2010 bei den Wohnungs- und Gebäudeei-

gentümern decken. Die Rechtsgrundlage für diese auch Zensus-Vorinformation genannte Vorerhebung findet sich in § 6 Abs. 1 Nr. 1 BStatG. Dort heißt es, dass „… zur Vorbereitung und Durchführung durch Rechtsvorschrift angeordneter Bundesstatistiken 1. zur Klärung des Kreises der zu Befragenden und deren statistischer Zuordnung Angaben …“ erhoben werden können.
Wichtigstes Indiz dafür, dass eine vom Statistischen Landesamt für den Eigentümer gehaltene Person nicht der wirklich Auskunftspflichtige sein könnte, war die Nichtzustellbarkeit der Erhebungsunterlagen auf dem Postweg. Die Adressen auf den nicht zustellbaren Unterlagen wurden durch die Deutsche Post AG dem Statistischen Landesamt mitgeteilt, das in diesen Fällen die tatsächlichen Auskunftspflichtigen zu ermitteln versuchte. Außerdem hatten die angeschriebenen Personen, die für das betreffende Gebäude und die darin befindlichen Wohnungen keine Angaben oder, z. B. wegen Verkauf der Immobilie, keine Angaben mehr machen konnten, die Möglichkeit, die statt dessen auskunftsfähigen Personen anzugeben.
Mindestens genauso wichtig, wie die auskunftsfähigen Personen zu kennen, war für das Statistische Landesamt, deren statistische Zuordnung zu erfahren. Der Grund dafür lag nicht zuletzt in der Gemeindegebietsreform in Sachsen-Anhalt. Zu den Jahren 2007 bis 2011 hatte sich die Zahl der Gemeinden in Sachsen-Anhalt durch freiwillige Zusammenschlüsse oder Zuordnungen von 1.033 auf 219 reduziert. Dadurch waren unter Umständen Gemeindenamen und in den Gemeinden Straßennamen zu ändern. Der Versuch des Statistischen Landesamtes, dort Klarheit zu schaffen, diente dem Ziel, die Menge der nicht oder an falsche Personen zustellbaren Erhebungsunterlagen beim eigentlichen Zensus 2011 möglichst gering zu halten. Der Stichtag für den Zensus 2011 war der 9. Mai 2011.

Natürlich hat der Landesbeauftragte den Vorbereitungsprozess des Zensus 2011 auch im zurückliegenden Berichtszeitraum eng begleitet. Allerdings hatte die Tatsache, dass Anfragen des Landesbeauftragten zum Zensus 2011 an das Statistische Landesamt und an das Ministerium des Innern als für die Statistik zuständiger oberster Aufsichtsbehörde zuweilen zäh und schleppend und mitunter auch unvollständig beantwortet wurden, seine Arbeit nicht erleichtert.

Der Landesbeauftragte prüft im Übrigen im Verlauf des Zensus mehrere Erhebungsstellen hinsichtlich der Beachtung des statistikrechtlichen Trennungsgebots.

23.1.1 Das Zensusausführungsgesetz des Landes Sachsen-Anhalt

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 22.1) über die wesentlichen Schritte der Erarbeitung eines (Bundes-)Zensusgesetzes und die datenschutzrechtlichen Kritikpunkte bereits berichtet. Durch das Inkrafttreten dieses Gesetzes am 16. Juli 2009 (BGBl. I S. 1781) war der Rahmen bestimmt worden, in dem ein entsprechendes Landesgesetz die Umsetzung des Zensusgesetzes 2011 für Sachsen-Anhalt zu bestimmen hatte.

Ein erster Entwurf eines Ausführungsgesetzes zum ZensG 2011 war dem Landesbeauftragten im November 2009 im Rahmen der Anhörung zugeleitet worden. Das Gesetz sollte im Wesentlichen die Arbeit der Erhebungsstellen

und der Erhebungsbeauftragten regeln. Der Landesbeauftragte hatte dem Ministerium des Innern daraufhin in einer dezidierten Stellungnahme verschiedene datenschutzrechtlich verbesserungswürdige Punkte genannt und Vorschläge zur Änderung unterbreitet, die auch teilweise übernommen wurden.
So hatte er z. B. Anstoß an § 7 Abs. 3 des Gesetzentwurfes genommen, der die Pflicht zur Übernahme der Tätigkeit als Erhebungsbeauftragter beim Zensus 2011 für Jedermann bestimmte. Mit der Vorschrift sollte § 11 Abs. 2 ZensG 2011 umgesetzt werden, sie ging jedoch weit darüber hinaus. § 11 Abs. 2 ZensG 2011 bestimmt nämlich, dass von Bund und Ländern benannte Bedienstete eine Tätigkeit als Erhebungsbeauftragte zu übernehmen haben. Der vom Landesbeauftragten kritisierte § 7 Abs. 3 des Gesetzentwurfes bezog jedoch „alle Bürger, die das 18. Lebensjahr vollendet haben“, in die Verpflichtung ein. Der Landesbeauftragte warnte davor, dass die Arbeitsergebnisse von quasi unter Androhung von Zwangsmaßnahmen von der Straße weg zu Erhebungsbeauftragten verpflichteten zu wünschen übrig lassen könnten und riet dazu, sich an den vom ZensG 2011 gesetzten Rahmen zu halten. Dieser Empfehlung wurde leider nicht gefolgt, wie § 6 Abs. 3 ZensAG LSA später zeigen sollte.

Ein anderer datenschutzrechtlich viel bedenklicherer Schauplatz tat sich dem Landesbeauftragten kurz nach der Abgabe seiner Stellungnahme auf. Ihm wurde nämlich durch den Datenschutzbeauftragten eines anderen Bundeslandes bekannt, dass Sachsen-Anhalt beabsichtige, einen Teil der im Zusammenhang mit dem Zensus 2011 zu erledigenden statistischen Arbeiten von gewerblichen Dienstleistern erbringen zu lassen (vgl. hierzu Nr. 23.1.2). Ein Hinweis, dass dies beabsichtigt sei, fehlte im E-ZensAG LSA jedoch zunächst. Zwar sieht § 17 Abs. 1 StatG-LSA, das ergänzend zum BStatG auch für die Durchführung von Bundesstatistiken gilt, vor, dass einzelne statistische Arbeiten an Dritte übertragen werden können. Der Landesbeauftragte verlangte jedoch, dass in das ZensAG LSA ein Hinweis auf diese Möglichkeit zur Aufgabenübertragung aufgenommen wird, um bei den betroffenen Bürgerinnen und Bürgern für mehr Transparenz zu sorgen. Dies wurde in § 1 Abs. 3 ZensAG LSA so auch Gesetzeswirklichkeit, nachdem zunächst eine intensive Diskussion zwischen dem Ministerium des Innern und dem Landesbeauftragten und zudem im Innenausschuss des Landtages geführt worden war.
Das ZensAG LSA trat schließlich am 15. Juli 2010 in Kraft (GVBl. LSA S. 422).

23.1.2 Übertragung einzelner statistischer Arbeiten an Dritte

Unter Nr. 23.1.1 hatte der Landesbeauftragte bereits über die Möglichkeit für die amtliche Statistik berichtet, unter bestimmten Voraussetzungen einzelne statistische Arbeiten an Dritte zu übertragen; wohlgemerkt: „einzelne Arbeiten“, so § 17 Abs. 1 StatG-LSA. Von dieser Möglichkeit macht man im Statistischen Landesamt bei der Durchführung des Zensus 2011 Gebrauch. Allerdings hat der Landesbeauftragte nach wie vor nicht restlos ausgeräumte Bedenken, dass es sich bei den zum Outsourcing vorgesehenen Arbeiten

- Personalisierung/Produktion und Versand der Erhebungsbögen für die Vorerhebung (vgl. Nr. 23.1) und die Gebäude- und Wohnungszählung als Bestandteil des Zensus 2011,

- Wiederentgegennahme und Aufbereitung zur Digitalisierung der genannten Erhebungsbögen, auch für die Haushaltsstichprobe und die Erhebung an Anschriften mit Sonderbereichen,

- Digitalisierung dieser Erhebungsbögen,

- Lesefehlerkorrektur einschließlich Deutung von Unklarheiten,

- Bereitstellung der gescannten Erhebungsbögen im Onlineverfahren für den Auftraggeber,

- Bereitstellung der einzelnen Datensätze und letztlich

- die Vernichtung der gescannten Erhebungsbögen

zwar prinzipiell um einzelne statistische Arbeiten handelt, aber eigentlich eine Übertragung eines erheblichen Teils des Zensus 2011 auf gewerbliche Dritte vorliegt. Der Landesbeauftragte bezweifelt, dass der Gesetzgeber dies so beabsichtigt hatte.

Die Aufträge sind erteilt, ein Teil davon im Berichtszeitraum bereits erbracht, bisher ohne dem Landesbeauftragten bekannt gewordene Datenschutzprobleme.
Die Personalisierung der Erhebungsbögen, also das Aufdrucken der Namen der Auskunftspflichtigen für die Vorerhebung zur Wohnungs- und Gebäudezählung (vgl. Nr. 23.1) und die Wohnungs- und Gebäudezählung im Rahmen des Zensus 2011 wurde durch die Deutsche Post AG erledigt, die das Ausschreibungsverfahren gewann. Sicherlich waren neben den wirtschaftlichen Gesichtspunkten auch Zusicherungen der Deutschen Post AG zur Gewährleistung des Datenschutzes, flankiert durch diverse technisch-organisatorische Maßnahmen, zur Entscheidungsfindung herangezogen worden. Gleichwohl bleibt nicht zu übersehen, dass der Dienstleister Deutsche Post AG bzw. seine involvierten Tochterunternehmen, ausgestattet mit einer Liste aller deutschen Wohnungs- und Wohngebäudeeigentümer, in einem seiner Geschäftsfelder allerlei Dienstleistungen rund um Adresshandel und -vermietung anbietet. Der Landesbeauftragte hatte nachdrücklich dafür gesorgt, dass die Deutsche Post AG sich vertraglich dazu verpflichtet, den überlassenen Datenbestand ausschließlich für die Erfüllung des Druckauftrages zu verwenden und jede weitere Nutzung unterbleibt.

Die Weiterbearbeitung der rücklaufenden Erhebungsbögen des Zensus 2011 erledigt ein Bayerisches Dienstleistungsunternehmen, das, seit Jahren bewährt in der Bearbeitung sensibler Datenbestände für öffentliche Auftraggeber, die Digitalisierung der für den Zensus 2011 gemachten Einzelangaben vornimmt. Die Angaben werden dem Statistischen Landesamt Sachsen-Anhalt zur Plausibilitätskontrolle übermittelt, danach die Erhebungsbögen vernichtet und beim Dienstleister die gespeicherten Daten gelöscht.

23.1.3 Mangelnde Transparenz

Wie in Nr. 23.1.2 berichtet, wird in Sachsen-Anhalt und auch in einigen anderen Bundesländern eine Fülle statistischer Arbeiten zur Vorbereitung und bei der Durchführung des Zensus 2011 an gewerbliche Dritte übertragen. Diese Übertragung rechtskonform abzuwickeln mag dem Statistischen Landesamt gemeinsam mit dem Ministerium des Innern gelungen sein. Mit dem Aufnehmen des vom Landesbeauftragten zur Verbesserung der Transparenz des Verwaltungshandelns geforderten Verweises im ZensAG LSA auf § 17 StatG-LSA (vgl. Nr. 23.1.1) sollte eine solche Auftragsvergabe prinzipiell möglich geworden sein.

Zu den übertragenen Arbeiten zählen bekanntlich auch die Wiederentgegennahme und die Aufbereitung der Erhebungsbögen der Vorerhebung zur Digitalisierung bei einem bayrischen Dienstleister, an den sie durch die Auskunftspflichtigen mittels Rücksendeumschlägen gesandt wurden. Ab Mai 2011 galt dies auch für die Erhebungsbögen der Gebäude- und Wohnungszählung im Rahmen des Zensus 2011.
Allerdings waren das Ministerium des Innern und das Statistische Landesamt zunächst der Meinung, dass es im Interesse eines reibungslosen Ablaufes des Zensus 2011 wohl besser wäre, wenn die Auskunftspflichtigen von der Beauftragung gewerblicher Dritter nicht unterrichtet würden. So war – wie dem Landesbeauftragten bekannt wurde – bis Mitte des Jahres 2010 tatsächlich beabsichtigt, auf den Rücksendeumschlägen für die Vorerhebung zum Zensus 2011 und für die Gebäude- und Wohnungszählung ausschließlich das Statistische Landesamt als Adressat anzugeben, obgleich die Briefe, gesteuert durch die Postfachnummer, direkt an den Bayerischen Auftragnehmer gehen sollten. Der Landesbeauftragte hat daraufhin die öffentliche Anhörung zum Entwurf eines ZensAG LSA (vgl. Nr. 23.1.1) im Ausschuss für Inneres des Landtages genutzt und für mehr Transparenz gegenüber den Auskunftspflichtigen geworben. Schließlich ist bereits dem legendären Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 zu entnehmen, dass der Einzelne ein Recht darauf hat zu wissen, wer was wann bei welcher Gelegenheit über ihn weiß. Durch das Ministerium des Innern wurde in der Anhörung deutlich gemacht, dass es die Hinweise des Landesbeauftragten zur Transparenz gegenüber dem Bürger „sehr ernst“ nehme. Man wolle auch die Empfehlung des Landesbeauftragten aufgreifen und die eingangs benannten Erhebungsbögen gemeinsam mit einer Art Beipackzettel an die Auskunftspflichtigen versenden, der auch Erläuterungen in Bezug auf die Vergabe statistischer Arbeiten an Dienstleister enthalten solle.

Allerdings war davon zunächst nicht viel zu spüren. Der Landesbeauftragte setzte im Ergebnis umfangreicher Erörterungen schließlich durch, dass als Adressaufdruck auf den Rücksendeumschlägen folgendes erscheint:

> Systemform MediaCard GmbH – Beleglesezentrum
> im Auftrag des Statistischen Landesamtes Sachsen-Anhalt
> Postfach
> PLZ Hallstadt

Nur diese Art der Adresse entspricht dem Anspruch der Auskunftspflichtigen auf volle Transparenz, wer wo mit ihren Daten in Kontakt kommt.

Der Landesbeauftragte kontrollierte bei diesem Unternehmen Einzelaspekte der Datensicherheit; Anlässe für Beanstandungen fanden sich nicht.

Der Erläuterungsbogen zum Erhebungsbogen der Vorerhebung sollte, so hatte das Ministerium des Innern im Innenausschuss schließlich verlauten lassen, Hinweise geben zu der auf dem Rücksendeumschlag angegebenen Bayerischen Dienstleisteradresse. Diese Hinweise waren jedoch so wenig aussagekräftig, dass das Statistische Landesamt und auch den Landesbeauftragten während der Vorerhebung eine Fülle von Nachfragen irritierter Bürgerinnen und Bürger zur Rücksendeadresse erreichten.
Der Landesbeauftragte machte deshalb konkrete Formulierungsvorschläge für den Erläuterungsbogen zur im Mai 2011 stattfindenden Gebäude- und Wohnungszählung im Rahmen des Zensus 2011, die so durch das Statistische Landesamt auch angenommen und an den Druckdienstleister übermittelt worden waren.

23.1.4 Übermittlungssperren

Wesentlicher Teil des Zensus 2011 ist die Haushaltsbefragung auf Stichprobenbasis nach § 7 ZensG 2011, die sog. Haushaltsstichprobe. Die Auswahl erfolgt „… geschichtet nach einem mathematischen Zufallsverfahren auf der Grundlage des Anschriften- und Gebäuderegisters“. Der Stichprobenumfang soll dabei 10% der Bevölkerung nicht überschreiten, so das Gesetz.
Bei diesem Verfahren drängt sich förmlich der Vergleich mit dem Mikrozensus (vgl. Nrn. 23.2 und 23.2.1) auf, doch es gibt erhebliche Unterschiede: Während beim Mikrozensus Auswahlbezirke bestimmt werden, in denen befragt wird, sind es beim Zensus 2011 Anschriften mit Wohnraum (§ 7 Abs. 3 ZensG 2011) aus dem Anschriften- und Gebäuderegister. Alle Personen an einer solchen Anschrift sind auskunftspflichtig. Die Erhebungsbeauftragten bzw. Interviewer erhalten nach § 11 Abs. 11 ZensG 2011 zur Unterstützung ihrer Tätigkeit bei der Erhebung einen verkürzten Melderegisterauszug für die betreffenden Anschriften. Dieser Auszug enthält für die unter der Anschrift gemeldeten Personen die Angaben zu Familienname, Vornamen, Geschlecht, Tag der Geburt, Staatsangehörigkeit und natürlich Angaben zur Anschrift. Bei diesem Melderegisterauszug, eigentlich einer Liste der gemeldeten Bewohner, und dem Verfahren der Befragung „an einer Anschrift“ liegt der Hase im Pfeffer.
Nach § 3 ZensG 2011 haben die Meldebehörden dem Statistischen Landesamt und dieses dem Statistischen Bundesamt eine Fülle von Melderegisterdaten jedes einzelnen Einwohners zu übermitteln. Diese Melderegisterdaten werden vom Statistischen Bundesamt im Meldedatenregister gespeichert, also in einem datenschutzrechtlich eigentlich hoch problematischen zentralen Einwohnerregister. Dessen Aufgabe ist zwar auf den Zensus 2011 beschränkt und mit dem in Nr. 5.3 des I. Tätigkeitsberichts des Landesbeauftragten beschriebenen zentralen Einwohnerregister der ehemaligen DDR nicht vergleichbar, gleichwohl birgt es erhebliche Risiken. In diesem Register nämlich sind nicht nur die Daten der Einwohner gespeichert, für die eine melderechtliche Auskunfts- bzw. Übermittlungssperre nach § 35 Abs. 2 MG LSA eingerichtet ist, z. B. weil für sie durch eine Melderegisterauskunft eine Gefahr für Leben oder Gesundheit bestände. Außerdem sind in dem Register für diese Einwohner nach § 3 Abs. 1 Nr. 26 ZensG 2011 auch die Tatsache, dass eine Übermittlungssperre besteht, und sogar der Grund der

Übermittlungssperre gespeichert. Mit einem im Übrigen die Tatsache gegebenenfalls bestehender Übermittlungssperren nicht enthaltenen Auszug aus diesem Register ausgestattet sollen nach dem Gesetz die Erhebungsbeauftragten die Daten zur Haushaltsstichprobe bei den Bürgerinnen und Bürgern erheben. Dadurch wäre es prinzipiell möglich, dass ein Erhebungsbeauftragter bei seiner Tätigkeit einer Person im Zeugenschutzprogramm oder einem verdeckten Ermittler gegenüber steht und, mit dem Gesetz im Rücken, Auskünfte begehrt.
Um dieses Problem zu entschärfen, sind verschiedene Szenarien denkbar, an deren Diskussion sich der Landesbeauftragte intensiv beteiligte:

1. Ersatzadressen

   Die Variante, der aus datenschutzrechtlicher Sicht uneingeschränkt der Vorzug zu geben wäre, ist der Austausch der Adressen, an denen Personen mit Auskunftssperre gemeldet sind, gegen Ersatzadressen. Allerdings wird diese Variante vom Bundesministerium des Innern und vom Statistischen Bundesamt aus statistikfachlicher Sicht abgelehnt. Es sei unter anderem denkbar, dass sich hinter einer solchen Adresse ein Hochhaus verbirgt und eine adäquate Ersatzadresse mit genügend Auskunftspflichtigen nicht zu finden wäre.

2. Nichtbefragung ausschließlich der auskunftsgesperrten Personen

   Die Nichtbefragung ausschließlich der Personen, für die eine Auskunftssperre eingetragen ist, wohl aber der anderen Personen in diesem Haushalt, wäre aus datenschutzrechtlicher Sicht abzulehnen. Der Erhebungsbeauftragte, ausgerüstet womöglich mit einer Negativliste der Auskunftsgesperrten, stellt beim Interview fest, dass ihm im Kreis der anwesenden Haushaltsmitglieder ein Auskunftsgesperrter gegenüber steht. Er müsste das Interview bei dieser Person beenden, nicht aber bei den anderen Personen, die dadurch evtl. erst von der Sonderbehandlung bzw. dem Sonderstatus des Betroffenen erfahren würden.
   Selbst die Tatsache, dass der Erhebungsbeauftragte bei dieser Variante über eine Negativliste der Auskunftsgesperrten verfügte, hielte der Landesbeauftragte für bedenklich.

3. Haushaltsherausnahmen

   Da der Erhebungsbeauftragte erst bei der ersten Kontaktaufnahme feststellt, in welchem Haushalt welche Personen leben, ist diese Variante aus dem unter 2. genannten Gründen ebenfalls abzulehnen.

4. Befragung aller an der Auswahladresse angetroffenen Personen

   Ist in der Erhebungsstelle und damit dem Erhebungsbeauftragten überhaupt nicht bekannt, an welcher Adresse Personen mit Auskunftssperre gemeldet sind und alle Angetroffenen bei der Haushaltsstichprobe werden befragt, könnte dies aus datenschutzrechtlicher Sicht ein tragbarer Kompromiss zwischen den Interessen der amtlichen Statistik und dem Schutz des Persönlichkeitsrechts der Betroffe-

nen darstellen. Die Erhebungsbeauftragten müssten, etwa durch Schulung, auf evtl. Konflikte vorbereitet sein. Die quasi inkognito unbekannten Auskunftsgesperrten verschwänden letztlich in der Anonymität der Masse. Sie hätten im Übrigen außerdem die Möglichkeit, ihrer Auskunftspflicht online oder durch Selbstausfüllung des Fragebogens nachzukommen.

Im Übrigen ist folgendes zu bedenken:
Selbst wenn die Auskunftsgesperrten aus der Haushaltsstichprobe völlig herausgenommen würden (s. oben Nrn. 1.-3.), würde doch nicht in jedem Fall zu verhindern sein, dass sie beim Zensus 2011 von Interviewern aufgesucht werden: Und zwar im Rahmen der Gebäude- und Wohnungszählung, zu der alle Haus- und Wohnungseigentümer heranzuziehen sind, unbeschadet einer melderechtlichen Auskunftssperre. Erhebungsbeauftragte würden dann vorstellig werden, wenn zur Klärung von Unstimmigkeiten eine Befragung nach § 16 ZensG 2011 erforderlich wird, oder zur Wahrnehmung ihrer Aufgaben nach § 11 Abs. 5 i. V. m. § 6 ZensG 2011. Bei diesen Aufgaben handelt es sich bezeichnenderweise gerade um die Feststellung der Auskunftspflichtigen für die Gebäude- und Wohnungszählung und bei fehlenden, unvollständigen oder widersprüchlichen Antworten.

Der Landesbeauftragte präferierte vor dem Hintergrund der Ablehnung der Variante 1 durch die amtliche Statistik die Variante 4 und teilte dies dem Ministerium des Innern und dem Statistischen Landesamt anlässlich einer Beratung im Januar 2011 auch so mit. In der Praxis wird bundeseinheitlich so verfahren.
Zusätzlich wurde besprochen, dass die Sicherheitsbehörden über eine mögliche Befragung der betroffenen Personen im Rahmen der Haushaltsstichprobe informiert werden.

23.1.5 Verschiedene Ordnungsnummernsysteme

Dass es in einer so umfangreichen Statistik – immerhin geht es um die Verarbeitung der Daten von rund 82 Millionen Menschen und ihrer Wohnungen – nicht ohne die Unterstützung durch hochleistungsfähige Computersysteme geht, liegt auf der Hand. Das Verknüpfen von Datensätzen, z. B. im Meldedatenregister mit solchen im Anschriften- und Gebäuderegister, von Datensätzen der Stichprobenorganisationsdatei mit solchen im Meldedatenregister oder einfach von Fragebögen mit den dahinter stehenden Auskunftspflichtigen bedarf jedoch zusätzlich verschiedener Ordnungsnummernsysteme.
Der Landesbeauftragte hat die beim Zensus 2011 verwendeten Ordnungsnummernsysteme argwöhnisch beobachtet, gilt doch der vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz aus dem Jahre 1983 aufgestellte Grundsatz, dass die Einführung eines einheitlichen Personenkennzeichnens als entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, abzulehnen sei. Deshalb kommen mehrere auf die unterschiedlichen statistischen Aufgaben speziell zugeschnittene Ordnungsnummernsysteme zur Anwendung.

Folgende Ordnungsnummernsysteme, so ist dem Landesbeauftragten durch das Ministerium des Innern und das Statistische Landesamt mitgeteilt worden, finden beim Zensus 2011 Verwendung:

1. PON – Personenbezogene Ordnungsnummer

   Die PON kann 30 bis 55 Stellen lang sein. Sie wird aus Geburtsname, Vornamen, Geburtsdatum, Geschlecht, Geburtsort und einem unterschiedlich langen variablen Teil gebildet. Nach der Bildung wird die PON verschlüsselt und anschließend in dieser verschlüsselten Form und ausschließlich statistikintern verwendet. Die PON ermöglicht eine Identifikation von Personen auf Anschriftenebene. Damit wird eine Zusammenführung der zu unterschiedlichen Zeitpunkten stattfindenden Datenanlieferungen aus den Melderegistern möglich.
   Rechtsgrundlage ist § 13 ZensG 2011.

2. AID – Identifikationsnummer des Auskunftspflichtigen bei der Gebäude- und Wohnungszählung im Zensus 2011

   Die AID identifiziert einen Auskunftspflichtigen nach Name bzw. Bezeichnung und Anschrift. Sie setzt sich aus einer 9-stelligen laufenden Nummer und einer Prüfziffer zusammen. Die Vergabe erfolgt durch das Statistische Bundesamt fortlaufend für das gesamte Bundesgebiet.
   Mit der AID wird ein Auskunftspflichtiger einem oder bei Großeigentümern mehreren Gebäuden oder Wohnungen zugeordnet. Ziel soll sein, dass zu jedem Gebäude im Anschriften- und Gebäuderegister mindestens ein Auskunftspflichtiger zugeordnet ist. Die AID wird nur statistikintern verwendet.

3. Ordnungsnummer der Meldebehörden

   Diese zu jedem gemeldeten Einwohner im Melderegister zu führende Nummer ist gem. § 3 Abs. 1 Nr. 1 ZensG 2011 von den Meldebehörden an die Statistischen Landesämter und von diesen an das Statistische Bundesamt zu übermitteln. Sie dient der Unterscheidung von Personen.
   Die Ordnungsnummer der Meldebehörden wird auch OMP – Ordnungsmerkmal der Person – genannt.

4. Ordnungsnummern

   Für jede Anschrift, jedes Gebäude, jede Wohnung, jeden Haushalt und jede Person wird von den Statistischen Ämtern des Bundes und der Länder gem. § 13 ZensG 2011 eine Ordnungsnummer vergeben und geführt. Diese Ordnungsnummern können bei den verschiedenen Zusammenführungen der Datensätze aus unterschiedlichen Registern nach § 9 verwendet werden. Sie müssen spätestens am 9. Mai 2015 gelöscht sein.

5. BKZ – Belegkennzeichen

   Das BKZ ist 38 Stellen lang und wird in der vorletzten Zeile jedes Fragebogens als Zahl und zur maschinellen Belegerkennung und -lesung in der letzten Zeile als Barcode gedruckt.
   Es enthält neben einer Angabe zur Fragebogenart, einer laufenden

Nummer jeder Seite des Fragebogens und einem Länderkennzeichen u. a. den Berichtseinheitenschlüssel. Der Berichtseinheitenschlüssel ist die 12 Stellen lange Fragebogennummer.

6. Fragebogennummer/Berichtseinheitenschlüssel

   Diese 12-stellige Nummer, die Teil des Belegkennzeichens ist und auch Berichtseinheitenschlüssel genannt wird, dient der Identifikation des Auskunftspflichtigen, wenn dieser von der Möglichkeit Gebrauch macht, seine Auskünfte über die offizielle Website des Statistischen Bundesamtes zum Zensus 2011 unter http://www.zensus2011.de online zu erteilen.

23.1.6 Datenübermittlung an kommunale Statistikstellen

Der Zensus 2011 als Statistik ist nicht Selbstzweck. Vielmehr hat der Bundesgesetzgeber auch vorgesehen, dass die Statistischen Ämter des Bundes und der Länder den Gemeinden und Gemeindeverbänden auf Ersuchen für deren Zuständigkeitsbereich Einzelangaben aus den Erhebungen des Zensus 2011 übermitteln dürfen. Eine solche Regelung, bei der Einzelangaben aus dem abgeschotteten Bereich der Statistik in den Verwaltungsvollzug gelangten, spräche Datenschutz und statistischer Geheimhaltung Hohn, wäre sie nicht durch Einschränkungen bewehrt. Nach § 22 Abs. 2 ZensG 2011 dürfen die Einzelangaben nämlich nicht in den Verwaltungsvollzug übermittelt werden, sondern nur an die ausschließlich für statistische Aufgaben zuständigen Stellen. Das sind die kommunalen Statistikstellen, deren räumliche und organisatorische Trennung von den anderen Verwaltungsstellen in § 7 StatG-LSA vorgeschrieben ist. In Sachsen-Anhalt existieren z. Zt. sieben kommunale Statistikstellen, die Adressaten einer solchen Datenübermittlung sein könnten.

Außerdem hat der Gesetzgeber bestimmt, dass zu den Erhebungsmerkmalen nur die Hilfsmerkmale Straße und Hausnummer bereitgestellt werden dürfen. Da dies in vielen Fällen immer noch personenbeziehbar wäre, wurde außerdem normiert, dass die Hilfsmerkmale zum frühestmöglichen Zeitpunkt, spätestens jedoch zwei Jahre nach der Übermittlung, zu löschen sind (vgl. § 22 Abs. 2 Satz 3 ZensG 2011).

Die Gemeinden und Gemeindeverbände hätten auch die Möglichkeit, sich nach Blockseiten zusammengefasste Einzelangaben, jedoch ohne weitere Hilfsmerkmale, übermitteln zu lassen, die sie dann dauerhaft speichern dürften. Auch das könnte jedoch datenschutzrechtlich problematisch sein. Zur Frage der Blockseiten und ihrer Bildung muss man folgendes wissen: Eine Blockseite ist nach § 10 Abs. 3 BStatG eine Seite mit gleicher Straßenbezeichnung von der durch Straßeneinmündungen oder vergleichbare Begrenzungen umschlossenen Fläche. Das könnte – datenschutzrechtlich unverfänglich – ein langer Häuserblock zwischen angrenzenden Straßen sein oder aber ein einzeln stehendes nur von einer Person bewohntes Haus. Damit genau dies nicht passiert, die aggregierten Daten einer Blockseite womöglich doch personenbeziehbar wären, hat der Landesbeauftragte bereits Kontakt mit dem Ministerium des Innern und dem Statistischen Landesamt aufgenommen und darauf hingewirkt, dass Blockseiten so gebildet werden, dass

die Zahl der an einer Blockseite vorhandenen Einwohner bzw. Auskunftspflichtigen nicht zu gering ausfällt, wodurch eine unzulässige bzw. ungewollte Deanonymisierung ausgeschlossen wäre.

23.2 Mikrozensus

Der Mikrozensus ist eine amtliche Statistik, die bundesgesetzlich angeordnet worden ist. Über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte, so heißt es im Mikrozensusgesetz 2005, werden Erhebungen auf repräsentativer Grundlage (Mikrozensus) als Bundesstatistik durchgeführt. Zweck des Mikrozensus ist es, statistische Angaben über die Bevölkerungsstruktur, die wirtschaftliche und soziale Lage der Bevölkerung, der Familien und der Haushalte, den Arbeitsmarkt, die berufliche Gliederung und die Ausbildung der Erwerbsbevölkerung sowie die Wohnverhältnisse bereitzustellen.

Dabei ist die Bezeichnung Mikrozensus eigentlich irreführend, denn nicht jeder millionste Haushalt wird befragt, sondern jeder einhundertste, es handelt sich also um eine 1%-ige Stichprobe. Exakt übersetzt bedeutet Mikrozensus nämlich „kleine Volkszählung“. Wegen der Heranziehung von jährlich weit über 20.000 Bürgerinnen und Bürgern allein in Sachsen-Anhalt steht die Durchführung des Mikrozensus ständig im Blick des Landesbeauftragten. Grund zur Beanstandung hatte er dabei bisher nicht. Einzelne Teile des Erhebungsverfahrens zum Mikrozensus sollen hier näher erörtert werden.

23.2.1 Wie erfolgt die Auswahl der Auskunftspflichtigen?

Zur Beantwortung dieser Frage traten immer wieder Auskunftspflichtige mit der Bitte um Erläuterung des Verfahrens, gelegentlich auch gleich mit der Bitte um Abhilfe, an den Landesbeauftragten heran.
Ausgewählt vom Statistischen Bundesamt werden nicht etwa Namen von Personen, diese sind dem Amt gar nicht bekannt, sondern Flächen. Die Auswahl erfolgt nach einem mathematisch-statistischen Zufallsverfahren. Dazu wurde, so teilte das Statistische Bundesamt mit, das gesamte bewohnte Bundesgebiet auf Basis des Materials der Volkszählung von 1987 in Flächen, sogenannte Auswahlbezirke, unterteilt. Für die neuen Länder und Ostberlin wurde nach der deutschen Vereinigung das Bevölkerungsregister „Statistik“ für die Unterteilung genutzt.
Die Anzahl der Wohnungen in den Auswahlbezirken soll ungefähr gleich groß sein. Diese Auswahlbezirke bestehen je nach den dort angesiedelten Gebäudetypen aus mehreren Einfamilienhäusern, einzelnen Gebäuden mit mehreren Wohnungen oder aus Gebäudeteilen. Aus der Gesamtheit der Auswahlbezirke wurden 20 nach regionalen Variablen und nach dem Gebäudetyp geschichtete 1%ige Vorratsstichproben mit jeweils knapp 400.000 Haushalten gezogen. Alle Personen aus Privathaushalten und Gemeinschaftsunterkünften, die auf dem Gebiet eines sich in der Stichprobe befindlichen Auswahlbezirks wohnen, werden grundsätzlich befragt. Gebäude ab einer bestimmten Größe unterliegen dabei der Gebäudeteilung. Das heißt, es werden nur durch vorgeschriebene Teilungsregeln bestimmte Etagen einbezogen. Außerdem erfolgt jährlich auf der Basis der Bautätigkeitsstatistik eine Anpassung der Mikrozensusstichproben.
Jahr für Jahr wird ein Viertel der ausgewählten Haushalte durch andere er-

setzt, was bedeutet, dass ein Haushalt für vier aufeinander folgende Jahre in der Stichprobe verbleibt. Zunächst hat die amtliche Statistik noch keine Kenntnis darüber, in welchen Haushalten im Erhebungsgebiet welche Personen leben. Das wird erst mit dem erstmaligen Besuch des regionalen Erhebungsbeauftragten bekannt, der die Wohnungen im Erhebungsgebiet aufsucht und die darin vorhandenen Haushalte und die in diesen lebenden Personen feststellt. Aus erhebungssystematischen Gründen kann kein zum Mikrozensus herangezogener Haushalt und keine darin lebende Person gegen andere ausgetauscht werden.
Das Auswahlverfahren ist datenschutzrechtlich nicht zu beanstanden.

23.2.2 Auskunftspflicht

Die auf der Basis des Mikrozensusgesetzes 2005 erhobenen Daten zur Bevölkerung, ihrer Struktur und ihrer wirtschaftlichen und sozialen Lage, zu Familien und zu den Haushalten, zur Wohnsituation und den Wohnverhältnissen der Haushalte und zum Arbeitsmarkt, zur beruflichen Gliederung und zur Ausbildung der Erwerbsbevölkerung sind für die Aufgabenerfüllung von Politik und Verwaltung und für vielfältige planerische Zwecke auf allen politischen Ebenen von so immenser Bedeutung, dass der Gesetzgeber für fast alle Erhebungsmerkmale des Mikrozensus eine Auskunftspflicht festgelegt hat (§ 7 Abs. 1 Mikrozensusgesetz 2005).
Lediglich die Fragen nach einer bestehenden Wohn- und Lebensgemeinschaft, nach dem Bezug vermögenswirksamer Leistungen und deren Anlage, nach der Zahl der im Ausland lebenden Kinder von Ausländern, nach dem Bestehen und der Höhe einer Lebensversicherung, nach Krankheiten und Unfällen und einige wenige andere Fragen sind freiwillig zu beantworten.

23.2.3 Formen der Auskunftserteilung

Es gibt verschiedene Möglichkeiten der Auskunftserteilung. Die meisten Befragten entscheiden sich für ein persönliches Gespräch mit einem Erhebungsbeauftragten, der sich rechtzeitig vor seinem Besuch schriftlich ankündigt, natürlich ausweisen kann und die Antworten der Auskunftspflichtigen in einem besonders gesicherten dienstlichen Laptop eingibt. Die Auskunftspflichtigen haben auch die Möglichkeit, ihre Auskünfte dem Statistischen Landesamt telefonisch zu geben, was nur ca. 10 bis 15 Minuten dauern wird. Schließlich können die Auskunftspflichtigen auch einen Fragebogen selbst ausfüllen, den ihnen der Erhebungsbeauftragte übergibt.

23.2.4 Folgen der Auskunftsverweigerung trotz bestehender Auskunftspflicht

Nach § 9 Mikrozensusgesetz 2005 finden die Bußgeldvorschriften des BStatG, das sind die §§ 23 und 24, keine Anwendung. Wer jedoch glaubt, damit wären der amtlichen Statistik alle Mittel zur Durchsetzung der Auskunftspflicht genommen und er könne die wiederholten Erinnerungen und Bitten des Statistischen Landesamtes um Auskunft aussitzen, der irrt freilich. Statt des Bußgeldes wird ein Zwangsgeld angeordnet und auch verhängt. Rechtsgrundlage ist § 71 VwVG i. V. m. §§ 53 und 54 SOG LSA. Damit ist auch die wiederholte Verhängung eines Zwangsgeldes zur Durchsetzung der Auskunftspflicht möglich.

23.3 Mehrjährige Zugehörigkeit zu einer 15%-Stichprobe

Der Landesbeauftragte hatte im Rahmen seiner Zusammenarbeit mit den Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den anderen Bundesländern zuständig sind (vgl. § 22 Abs. 7 DSG-LSA), von einem interessanten Urteil des Sächsischen Oberverwaltungsgerichts vom 15. Januar 2010 – 3 B 45/07 – Kenntnis erlangt. Dieses Urteil zum Ermessen der Statistikbehörde am Beispiel des DlStatG, eine mehrjährige Stichprobenzugehörigkeit und eine daraus folgende Heranziehung zur Erfüllung der Auskunftspflicht zu bestimmen, könnte wegen der enthaltenen instruktiven Überlegungen auch für Sachsen-Anhalt von Interesse sein.

Nach § 1 Abs. 2 DlStatG umfasst die Dienstleistungsstatistik jährliche Erhebungen bei 15% aller Erhebungseinheiten, die nach mathematisch-statistischen Verfahren auszuwählen sind. Der klagende Unternehmer war mehrere Jahre in Folge in dieser 15%igen Stichprobe enthalten und fühlte sich durch das seiner Meinung nach über die Jahre seiner Stichprobenzugehörigkeit entstehende Persönlichkeitsprofil in seinen Persönlichkeitsrechten beeinträchtigt und benachteiligt. In Sachsen-Anhalt kann dies eigentlich nicht passieren, wenn sich das Statistische Landesamt an seine dem § 12 Abs. 1 BStatG entsprechende Verpflichtung hält, die Hilfsmerkmale der Dienstleistungsstatistik nach Abschluss der jährlichen Erhebung sofort zu vernichten (vgl. IX. Tätigkeitsbericht Nr. 22.2). Das Sächsische Oberverwaltungsgericht war wie der Datenschutzbeauftragte dieses Landes zu einem anderen Ergebnis gekommen als der betroffene Unternehmer, allerdings auf einem ganz anderen Wege als wegen der schnellen Abtrennung und Löschung der Hilfsmerkmale.

Die Unternehmen eines Wirtschaftszweiges werden, nach Größenklassen gestaffelt, in Schichten gruppiert. Bemessen an der Zahl der beschäftigten Personen und dem Umsatzgewicht wird nach mathematisch-statistischen Verfahren für jede einzelne Schicht der Auswahlsatz so festgelegt, dass für den Wirtschaftszweig insgesamt der vom Gesetzgeber geforderte Auswahlsatz von 15 % eingehalten wird. Statistisch erfasst wären dann Betriebe mit 15 % der Beschäftigten und mit 15 % des Gesamtumsatzes des Wirtschaftszweiges. Für einzelne gering besetzte Schichten kann das Ergebnis der Schichtung und Auswahl aber durchaus von der 15%-Vorgabe des Gesetzgebers wesentlich abweichen oder gar eine Vollerhebung sein.
Das Gericht beanstandete nicht, dass eine einmal gezogene Stichprobe über mehrere Jahre hinweg Verwendung findet, wenn sie jährlich um ca. 15 % der Neuzugänge des Wirtschaftszweiges angereichert wird; heißt es in § 1 Abs. 1 DlStatG doch, Zweck der Dienstleistungsstatistik sei die Darstellung der Entwicklung der wirtschaftlichen Tätigkeit im Dienstleistungsbereich. So könne statistisches Material in Form von Zeitreihen bereitgestellt werden, das eine Grundlage für Analysen des Strukturwandels in diesem Wirtschaftsbereich bildet, ohne Beeinflussung durch einen eventuellen Stichprobenfehler.
Vor dem Hintergrund der engen statistikrechtlichen Geheimhaltungsvorschriften sei dies aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Der Landesbeauftragte kommt allerdings zu einem datenschutzrechtlich durchaus nicht unbeachtlichen anderen Ergebnis. Das einer möglichen Auf-

wandersparnis und dem Ziel, Veränderungen der Wirtschaftstätigkeit im Dienstleistungsbereich über einen gewissen Zeitraum hinweg stichprobenfehlerfrei beobachten zu wollen, geschuldete mehrmalige Recycling einer einmal gezogenen Stichprobe, auch wenn sie regelmäßig ergänzt wird, könnte durchaus statistikmethodisch fehlerhaft sein: Wenn nämlich durch den oben beschriebenen Strukturwandel und die damit verbundenen Änderungen bei den in der Stichprobe bereits enthaltenen Unternehmen Beschäftigtenzahl und erzielter Umsatz der Gesamtstichprobe nach vieljähriger Verwendung die vom Gesetzgeber geforderten 15% von Beschäftigtenzahl und Gesamtumsatz nicht mehr abbildeten, könnte auch nach Ergänzungsziehungen zur Stichprobe aus den Neuzugängen das statistische Ergebnis verfälscht sein, womit die gesamte auskunftspflichtbewehrte Befragung ungeeignet und damit verfassungsrechtlich angreifbar wäre. Im Übrigen ist das herangezogene Ermessen der Statistikbehörde hinsichtlich der Befugnisnorm zur Datenerhebung nur auf Zweck und Auftrag der Dienstleistungsstatistik gestützt.

Der Landesbeauftragte empfiehlt dem Statistischen Landesamt Sachsen-Anhalt, bei der Ziehung von Stichproben nicht nur im Dienstleistungsbereich, einen möglichen Erkenntnisgewinn durch Verfolgung der wirtschaftlichen Entwicklung einer Unternehmensauswahl in langen Zeitreihen und die eventuell eintretende Kostenersparnis durch das Stichprobenrecycling hinter die Einhaltung des vom Gesetzgeber normierten Auswahlsatzes für die Stichprobe zurückzustellen.

23.4 Ethnische Minderheiten in der Geschäftsstatistik

Dem Landesbeauftragten war die Anfrage zugegangen, ob die Auswertung von Volkszugehörigkeiten, z. B. zu Sinti und Roma, im Rahmen einer Geschäftsstatistik der besonderen gesetzlichen Legitimation bedarf oder womöglich völlig unzulässig wäre.
Die Antwort darauf erschließt sich aus dem DSG-LSA und dem StatG-LSA.

In Sachsen-Anhalt werden personenbezogene Daten wie die Volkszugehörigkeit, also „Angaben über die rassische oder ethnische Herkunft“, als „personenbezogene Daten besonderer Art“ bezeichnet (vgl. § 2 Abs. 1 DSG-LSA). Sie dürfen nach § 26 Abs. 1 DSG-LSA u. a. nur dann zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erhoben, verarbeitet oder genutzt werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder der Betroffene eingewilligt hat.
Vor dem Hintergrund, dass einer Geschäftsstatistik nie eine Erhebung personenbezogener Daten nur zum Zweck dieser Statistik vorausgeht, weil die Daten eben bei der rechtmäßigen Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben angefallen sind, hat bereits dort die Prüfung der datenschutzrechtlichen Zulässigkeit des grundsätzlichen Umgangs mit diesen Daten besonderer Art einzusetzen. Sind die Daten im Verwaltungsvollzug tatsächlich erforderlich und nicht nur nützlich, um die Aufgabe zu erfüllen, und ist ihre Verwendung von einer Rechtsvorschrift vorgesehen oder hat der Betroffene eingewilligt, steht der Verwendung der personenbezogenen Daten besonderer Art auch zum Zweck der Erstellung einer Geschäftsstatistik nichts im Wege. Das StatG-LSA enthält für Geschäftsstatistiken (§ 5 StatG-LSA) keine Einschränkungen für die Nutzung auch von

personenbezogenen Daten besonderer Art. Das wird schließlich sinnfällig, wenn man beachtet, dass die verantwortliche Stelle durch das Aufstellen einer Geschäftsstatistik nicht zu Erkenntnissen im Einzelfall gelangt, die ihr nicht schon vorher aus dem Verwaltungsvollzug bekannt waren.

24 Strafvollzug

24.1 PPP-Projekt Justizvollzugsanstalt Burg – Entwicklung/Sachstand

In seinem VIII. und IX. Tätigkeitsbericht hatte der Landesbeauftragte bereits über die datenschutzrechtlichen Herausforderungen im Vorfeld des Baus und Betriebs der Justizvollzugsanstalt (JVA) Burg im Rahmen einer sog. Public-Private-Partnership (PPP) berichtet (Nr. 22.1. des VIII. und Nr. 23.1 des IX. Tätigkeitsberichts).

Im November 2009 hat die JVA Burg den Regelbetrieb aufgenommen. Die Verantwortung für den Strafvollzug verbleibt beim Staat. Der private Partner erbringt Dienstleistungen in einzelnen Fachbereichen. Hierzu gehören z. B. der Schreibdienst in der Verwaltung, die Besucherkontrolle, die Videoüberwachung von Besuchern und Gefangenen, der soziale Fachdienst, der u. a. für die psychologische Betreuung der Gefangenen zuständig ist, oder der Küchendienst, um nur einige Tätigkeitsfelder zu nennen. Bei dem privaten Partner handelt es sich um die Projektgesellschaft Justizvollzug Burg GmbH & Co KG, die zur Erfüllung ihrer Aufgaben Subunternehmer einsetzt, die unter Umständen weitere Subunternehmer beschäftigen. Mit dieser Aufgabenverteilung soll die JVA zu den sichersten und modernsten Anstalten in Europa gehören. Es ist bedauerlich, dass dieselben Ansprüche bisher nicht auch an den Datenschutz gestellt wurden: Obwohl es auf der Hand liegt, dass der private Dienstleister zur Erfüllung seiner Aufgaben sowohl die personenbezogenen Daten der Gefangenen als auch von Dritten, z. B. von den Besuchern, aber auch von den im Strafvollzug Beschäftigten erheben, nutzen und verarbeiten muss, weist das komplexe ca. 3.000 Seiten umfassende PPP-Vertragswerk unter datenschutzrechtlichen Gesichtspunkten erhebliche Defizite auf. So haben die Parteien bei Abschluss der Verträge offensichtlich übersehen, dass der private Dienstleister als Verwaltungshelfer Daten im Auftrag der staatlichen Stelle verarbeitet, da Regelungen zur Auftragsdatenverarbeitung im Vertragswerk weitgehend fehlen. Auch wird im Vertragswerk lediglich vereinzelt auf Fragen des Datenschutzes eingegangen. Die datenschutzrechtlichen Bestimmungen müssen dabei mehr oder weniger mosaikartig zusammengetragen werden. Regelungen für den Umgang mit personenbezogenen Daten an den Schnittstellen zwischen hoheitlichen und privaten Tätigkeiten sind weitgehend nicht vorhanden. Das derzeit für Sachsen-Anhalt geltende StVollzG ist in der Praxis keine Hilfe, da es Regelungen zur Auftragsdatenverarbeitung nicht enthält und in weiten Teilen modernisierungsbedürftig ist. Vor diesem Hintergrund hatte der Landesbeauftragte, der vor dem Abschluss der Verträge nicht beteiligt worden war, den Gesetzgeber aufgefordert, in einem zukünftigen Strafvollzugsgesetz des Landes Sachsen-Anhalt die Auftragsdatenverarbeitung gesetzlich zu regeln, und für den Betrieb der JVA Burg ein Datenschutzkonzept verlangt (IX. Tätigkeitsbericht Nrn. 23.1 und 23.2).

Aufgrund der Hinweise des Landesbeauftragten hat Sachsen-Anhalt für den Jugendstraf- und den Untersuchungshaftvollzug die Auftragsdatenverarbeitung gesetzlich geregelt (§ 106 Abs. 2 JStVollzG, § 97 UVollzG LSA). Allerdings steht die Aufnahme eines Erwachsenenstrafvollzugsgesetzes in das Landesrecht nach wie vor aus. Die neue Landesregierung will sich in der 6. Legislaturperiode dieser Problematik widmen. Damit wird der Einsatz privater Dienstleister im Erwachsenenstrafvollzug rechtlich vollständig abgesichert sein. Es ist allerdings bedauerlich, dass ein entsprechendes Gesetz nicht schon zum Zeitpunkt der Inbetriebnahme der JVA geschaffen wurde. Andere Bundesländer, wie z. B. Bayern, Baden-Württemberg und Niedersachsen, haben schon Erwachsenenstrafvollzugsgesetze erlassen. Bedauerlich ist auch, dass das Justizministerium das von ihm schon lange angekündigte Datenschutzkonzept weder rechtzeitig zur Aufnahme des Regelbetriebs noch zu dem Informations- und Kontrollbesuch des Landesbeauftragten vorlegen konnte (Nr. 24.2).

Es ist daher nicht weiter verwunderlich, dass nach der Inbetriebnahme der JVA Burg beim Landesbeauftragten auch bald die ersten datenschutzrechtlichen Beschwerden von Insassen zum Einsatz des privaten Dienstleisters insbesondere bei der Postkontrolle, der Verpflegung der Gefangenen und der Führung der Gefangenenpersonalakten eingingen. In diesem Zusammenhang ist festzuhalten, dass die Beschwerden, die meist nur zum Teil berechtigt waren, wesentlich schneller und zielgerechter hätten bearbeitet werden können, wenn sich die JVA Burg gegenüber dem Landesbeauftragten kooperativer gezeigt hätte. So war zur Aufklärung und Bewertung der Sach- und Rechtslage ein überdurchschnittlich hoher Schriftverkehr erforderlich. Ein weiterer Grund für die festzustellenden Verzögerungen dürfte sicherlich auch die Notwendigkeit der Einbeziehung des privaten Dienstleisters gewesen sein.

Die Beschwerden waren zugleich auch Gegenstand des Informations- und Kontrollbesuchs des Landesbeauftragten in der JVA Burg im Oktober 2010, bei dem die datenschutzrechtlich relevanten Schnittstellen zwischen dem Staat und dem privaten Dienstleister geprüft wurden (zu den Einzelheiten s. Nr. 24.2). Schwerpunktmäßig diente der Besuch der Information des Landesbeauftragten. Eine tiefergehende Kontrolle war dem Landesbeauftragten leider nicht möglich, da ihm ein vollständiges aktualisiertes Vertragswerk nicht rechtzeitig vorgelegt werden konnte. Der Besuch führte im Ergebnis zu einer Liste an datenschutzrechtlichen Mängeln und Verstößen, die sich angesichts des oben geschilderten Sachverhalts bereits im Vorfeld abgezeichnet hatten. Daher hätte durchaus Anlass für eine Beanstandung vorgelegen. Der Landesbeauftragte hat hierauf jedoch vorerst verzichtet, weil eine Beanstandung des Dauerzustands wenig sinnvoll gewesen wäre, zumal sich die Zusammenarbeit mit dem Justizministerium nach einer erfolgten Umstrukturierung erheblich verstärkt und verbessert hat. Das Ministerium hat bestätigt, dass noch Hausaufgaben zu machen seien.

Bemerkenswert ist die Feststellung der Justizministerin in einem Interview mit der Magdeburger Volksstimme vom 4. Februar 2011, in dem sie erklärt, dass es mit ihr ein Privatmodell nicht mehr geben werde, da dieses wegen der notwendigen Abstimmungen mit dem privaten Vertragspartner auf neue

Entwicklungen nicht so schnell reagieren könne, wie es bei herkömmlichen Haftanstalten möglich sei.

24.2 Informations- und Kontrollbesuch der JVA Burg

Im Oktober 2010 hat der Landesbeauftragte einen Informations- und Kontrollbesuch in der Justizvollzugsanstalt Burg (JVA Burg) durchgeführt, der im Ergebnis zeigte, dass für das Public-Private-Partnership-Projekt (PPP-Projekt) unter datenschutzrechtlichen Gesichtspunkten noch erheblicher Nachholbedarf besteht. Der Landesbeauftragte hat in seinem Prüfbericht datenschutzrechtliche Mängel und Probleme aufgezeigt, die es zu bewältigen gilt. Ein wesentlicher Aspekt ist z. B. die Ergänzung des PPP-Vertragswerks um Regelungen der Auftragsdatenverarbeitung und die Entwicklung eines Datenschutzkonzepts, das immer noch nicht vorliegt. Daneben müssen erkannte Mängel, wie z. B. die Durchsuchung von Besuchern durch den privaten Dienstleister, abgestellt werden.

Aber auch der Gesetzgeber ist gefragt, da das angekündigte Strafvollzugsgesetz des Landes Sachsen-Anhalt noch aussteht. Im Rahmen der Föderalismusreform ist durch das Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 (BGBl. I S. 2034) die Gesetzgebungskompetenz für den Strafvollzug, insbesondere der Vollzug der Freiheitsstrafe und der Jugendstrafe sowie der Untersuchungshaftvollzug, auf die Länder übertragen worden. Von seiner Gesetzgebungskompetenz hat der sachsen-anhaltische Gesetzgeber bereits durch Schaffung des JStVollzG LSA vom 7. Dezember 2007 (GVBl. LSA 2007 S. 368) sowie des UVollzG LSA vom 22. März 2010 (GVBl. LSA 2010 S. 157) Gebrauch gemacht. Im Erwachsenenstrafvollzug gilt bis zu einer landesrechtlichen Regelung, die noch aussteht, gem. Art. 125a Abs. 1 Satz 1 GG weiterhin das StVollzG, das in den §§ 179 ff. den Datenschutz abschließend regelt. An dieser Stelle muss noch einmal ausdrücklich darauf verwiesen werden, dass der Landesbeauftragte das Fehlen einer Rechtsgrundlage für die Auftragsdatenverarbeitung ausdrücklich bemängelt und den Rechtszustand bei der JVA Burg lediglich im Vorgriff auf die angekündigte Regelung im Erwachsenenstrafvollzug zur Auftragsdatenverarbeitung und die faktische Herstellung eines rechtskonformen Zustands toleriert hatte.

Der Erlass eines neuen Gesetzes ist aber auch deshalb notwendig, da im StVollzG bereichsspezifische Regelungen für datenverarbeitende Eingriffe weitgehend fehlen. So muss z. B. die Videoüberwachung zur Gewährleistung der Sicherheit der Justizvollzugsanstalten auf allgemeine Regelungen in den §§ 179 ff. StVollzG gestützt werden. Die Vorschriften zur Führung der Gefangenenpersonalakte sehen eine getrennte Aktenführung nur für die Krankenakten, nicht jedoch z. B. für die Therapieakten vor, sodass sie auch von Mitarbeitern eingesehen werden können, die diese Unterlagen zur Erfüllung ihrer Aufgaben gar nicht brauchen.

Anlass und Schwerpunkte des Besuchs

Der bereits in den Vorjahren avisierte Besuch war seit Beginn des Jahres 2010 in fünf Besprechungen mit dem Justizministerium, dabei zwei unter Beteiligung der JVA Burg sowie der privaten Dienstleister, vorbereitet worden.

Das komplexe Vertragswerk, die nicht immer leicht zu durchschauenden Auftrags- und Unterauftragsverhältnisse auf der Seite des privaten Dienstleisters und die unklare Struktur in den Verantwortlichkeiten hatte eine intensive Vorbereitung notwendig gemacht. Zum besseren Verständnis soll an dieser Stelle ein kurzer Überblick über die vorgefundenen Strukturen gegeben werden:

Vertragspartner sind das Land Sachsen-Anhalt und die Projektgesellschaft Justizvollzug Burg GmbH & Co. KG. Das Land wurde im Rahmen der Vertragsverhandlungen durch die Ministerien der Finanzen, der Justiz und für Landesentwicklung und Verkehr vertreten. Im Juni 2009 haben die Staatssekretäre der o. g. Ministerien die Zuständigkeiten für die Vereinbarung von Änderungen und Ergänzungen des PPP-Vertragswerks, die aus der Umsetzung des Vertrags resultieren, dem Leiter der JVA Burg übertragen. Der Landesbeauftragte hatte in den vergangenen Jahren beim Ministerium der Justiz mehrfach nach einer solchen Regelung nachgefragt. Diese bedeutsame Ermächtigung wurde ihm erst im Kontrolltermin durch die JVA Burg übergeben. Die Projektgesellschaft Justizvollzug Burg GmbH & Co. KG, die durch ihren Komplementär, die PJB-Management GmbH, vertreten wird, hat zur Erfüllung ihrer Pflichten Verträge mit Subunternehmen geschlossen, zu denen die Firma Kötter GmbH & Co. KG und die Firma HSG Zander GmbH gehören. Diese haben ihrerseits Subunternehmer eingeschaltet, die sich weiterer Subunternehmer bedienen.

Das komplexe ca. 3.000 Seiten umfassende Vertragswerk besteht aus einem Rahmenvertrag, einem PPP-Projektvertrag, einem Facility-Management-Vertrag und sieben Dienstleistungsverträgen (EDV-Systembetreuung, Gesundheitsfürsorge, Reinigung, Sicherheitshilfsdienste, Sozialfürsorge, Verpflegungsleistungen und Verwaltungshilfsdienste). Vertragsbestandteile sind ferner Unterhalts-, Betriebs- und Dienstleistungsbeschreibungen (UBD) zu den Dienstleistungsverträgen, sowie eine allgemeine Dienstanweisung nebst den bereichsbezogenen Dienstanweisungen für die einzelnen Dienstleistungsverträge. Teil der Verträge sind außerdem Service-Level-Agreements (SLA) sowie Konzepte zur Durchführung der Verträge. Darüber hinaus hat die JVA Burg selbst zusätzliche Hausverfügungen erlassen, die auch Auswirkungen auf die Datenverarbeitung staatlicher Beschäftigter und Mitarbeiter der privaten Dienstleister haben. Auf die Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten durch den privaten Dienstleister geht das Vertragswerk nur vereinzelt ein. Die entsprechenden Regelungen oder Anweisungen mussten mosaikartig zusammengesucht werden. Regelungen zur Auftragsdatenverarbeitung sind in dem Vertragswerk fast gar nicht enthalten.

Angesichts der im VIII. und IX. Tätigkeitsbericht dargestellten datenschutzrechtlichen Probleme und Mängel wurde für die Durchführung einer Kontrolle verabredet, vorab eine konsolidierte Fassung des Vertragswerks, das Datenschutzkonzept als Teil einer allgemeinen Dienstanweisung sowie den Entwurf einer vertraglichen Regelung zur Auftragsdatenverarbeitung zu übersenden. Dabei leistete der Landesbeauftragte bereits zu diesem Zeitpunkt eine über das übliche Maß hinausgehende Beratung und Hilfestellung. In den letzten Besprechungen musste das Ministerium der Justiz einräumen, dass eine Vorlage der gewünschten Unterlagen nicht rechtzeitig möglich sei. Vor diesem Hintergrund konnte der Kontrollbesuch schwerpunktmäßig nur informatorischen Charakter haben und musste sich auf bestimmte Bereiche be-

schränken. Näher betrachtet und kontrolliert wurden daher ausgewählte Schnittstellen zwischen hoheitlicher und nicht-hoheitlicher Datenverarbeitung. Im Folgenden soll auf einzelne Bereiche, in denen Mängel erkannt wurden, eingegangen werden.

Ausweiskontrolle und Durchsuchung von Besuchern durch den privaten Dienstleister

Mitarbeiter des privaten Dienstleisters führen an der Außenpforte die Ausweiskontrolle von Besuchern durch. An die Ausweiskontrolle schließt sich in einem besonderen Raum regelmäßig die körperliche Durchsuchung von Besuchern an. Die Übertragung der Durchsuchungsbefugnis auf den privaten Dienstleister war in den Verträgen nicht vorgesehen und ist am 3. Februar 2010 in der entsprechenden UBD erfolgt.

§ 155 StVollzG erlaubt zwar den Einsatz von Privaten als Verwaltungshelfer im Strafvollzug. Sie dürfen jedoch nur eingesetzt werden, sofern die Tätigkeit nicht mit der Ausübung von hoheitlichen Eingriffsbefugnissen bzw. der Ausübung von Zwangsbefugnissen verbunden ist. Der Einsatz Privater im Wege der Verwaltungshilfe kommt daher umso weniger in Betracht, je intensiver aufgrund potentieller Befugnisse in Grundrechte eingegriffen werden kann. Private sollen daher nur bei Dienst- oder Serviceleistungen (z. B. Küche) oder bei Überwachungsaufgaben ohne Ausübung von Gewalt (z. B. bei der Überwachung von Monitoren) eingesetzt werden können.

Da eine schlichte Ausweiskontrolle in dem Aushändigen und Überprüfen des Ausweises besteht, dürfte eine Übertragung dieser Aufgaben auf einen privaten Dienstleister wegen der Geringfügigkeit des Eingriffs im Ergebnis vertretbar sein. Dies kann jedoch nicht für die Durchsuchung gelten. Da nach ganz h. M. wegen der erhöhten Grundrechtsrelevanz schon eine Übertragung der Durchsuchung der Gefangenen auf private Dienstleister für unzulässig gehalten wird, erscheint eine Durchsuchung der Besucher durch private Dienstleister erst recht nicht möglich. Dies ist unabhängig von dem Umstand, dass in der JVA Burg keine Durchsuchung der Besucher im Intimbereich erfolgen soll und die Durchsuchung unter hoheitlicher Aufsicht erfolgt.

In seiner Stellungnahme zu den Ergebnissen des Prüfberichts argumentiert das Ministerium der Justiz, dass der private Dienstleister lediglich eine Absuchung durchführe, bei der es um eine unterstützende Maßnahme ohne Eingriffscharakter handele. Diese Auffassung ist nicht überzeugend, stellt doch die Absuchung, die z. B. das Abtasten oder das Absuchen einer Person mit technischen Hilfsmitteln wie z. B. Metalldetektoren erlaubt, lediglich einen Unterfall einer Durchsuchung dar. Angesichts der h. M. in Rechtsprechung und Lehre ist auch die Auffassung, dass die Ab- bzw. Durchsuchung der Besucher weder eine hoheitliche Tätigkeit beinhalte noch einen Eingriffscharakter besitze, nicht nachvollziehbar. Vielmehr findet sie nach der Rechtsprechung und Lehre ihre Rechtsgrundlage in § 24 Abs. 3 StVollzG und stellt einen erheblichen Eingriff in das Recht auf freie Entfaltung der Persönlichkeit dar. Eine Übertragung dieser Aufgabe auf den privaten Dienstleister ist daher nicht zulässig.

Videoüberwachung

Sofern eine Videoüberwachung erfolgt, muss üblicherweise auf sie durch Hinweisschilder aufmerksam gemacht werden. Die überwachende Stelle hat Festlegungen für dieses automatisierte Verfahren in einem Verfahrensverzeichnis zu führen, das von jedermann eingesehen werden kann. Die JVA Burg führt bisher kein entsprechendes Verzeichnis. Während die Besucher im Außenbereich durch Schilder auf die Videoüberwachung hingewiesen werden, fehlt eine entsprechende klare Beschilderung im Innenbereich. Stattdessen wird den Besuchern nur ein Merkblatt übergegeben, das auf die Videoüberwachung im Innenbereich einschließlich der Besucherräume hinweist.

Problematisch ist auch die Überwachung von Verteidigerbesuchen. § 27 Abs. 3 StVollzG bestimmt, dass sie nicht überwacht werden dürfen. Nach Angaben der JVA Burg wird bei dem Besuch des Verteidigers die automatische Videoüberwachung manuell gestoppt, sodass keine Überwachung mehr erfolgt. Dennoch bestehen gegenüber dieser Lösung Zweifel. Dadurch, dass sich in jedem Besuchsraum Kameras befinden, kann sich ein Verteidiger nicht sicher sein, ob nicht doch eine Überwachung durchgeführt wird. So kann z. B. nicht ausgeschlossen werden, dass durch ein Versehen die Unterbrechung der Videoüberwachung unterbleibt.

Der Landesbeauftragte hat daher empfohlen, Besucher auf die Videoüberwachung im Innenbereich deutlicher aufmerksam zu machen und spezielle Besucherräume nur für Verteidigerbesuche einzurichten, in denen sich keine Kameras befinden. Beiden Empfehlungen wurde nachgekommen.

Problematisch ist dagegen die Videoüberwachung besonders gesicherter Hafträume, die auch als sog. Beruhigungszellen bezeichnet werden. Eine Videoüberwachung dürfte zum Schutz des Gefangenen grundsätzlich zulässig sein, auch wenn die sanitäre Einrichtung einsehbar ist. Zweifelhaft ist aber, ob § 88 Abs. 2 Nr. 5 StVollzG eine hinreichende Rechtsgrundlage für die Videoüberwachung besonders gesicherter Hafträume darstellt. Kritisch ist auch, dass jeder Mitarbeiter bzw. jede Mitarbeiterin des privaten Dienstleisters, welche sich in der Sicherheitszentrale befinden, über Monitore die besonders gesicherten Hafträume einsehen können. Der Landesbeauftragte hatte daher die Prüfung empfohlen, ob die Videoaufzeichnung durch das mildere Mittel der optisch-elektronischen Beobachtung ersetzt werden könne und darum gebeten, dass die Videoüberwachung nur von Personen des gleichen Geschlechts durchgeführt wird. Das Justizministerium hält eine Videoüberwachung zum Schutz des Gefangenen wie zur Rekonstruktion von Vorgängen für nötig und hat angekündigt, eine hinreichende Rechtsgrundlage zu schaffen. Dagegen soll eine Überwachung der Betroffenen durch Personen des gleichen Geschlechts nicht möglich sein, da dies nur durch die Einrichtung eines gesonderten Arbeitsplatzes in einem geschlossenen Raum erreicht werden könnte. Diese Argumentation überzeugt jedoch nicht, da schon die Errichtung eines Blickschutzes als taugliche Schutzmaßnahme in Betracht käme, sofern es sich beim Überwachenden um eine Person des gleichen Geschlechts handelt.

Führung der Gefangenenpersonalakte und Einsicht durch die Fachdienste

In der JVA Burg werden die Gefangenenpersonalakten und die Therapieakten nicht getrennt geführt. Unter rechtlichen Gesichtspunkten ist dies vertretbar, da nach § 183 StVollzG i. V. m. Nr. 47 Abs. 4 der Vollzugsgeschäftsordnung bisher nur Krankenakten getrennt von der Gefangenpersonalakte geführt werden müssen. Eine getrennte Führung der Therapie- von der Gefangenenpersonalakte ist jedoch sinnvoll, da der Sachbearbeiter nicht notwendigerweise Kenntnis von den Therapiedaten haben muss.

Insofern war es als ein Fortschritt zu betrachten, dass die Justizministerin im Ausschuss für Recht und Verfassung des Landtages berichtet hatte, das Ministerium der Justiz habe dafür gesorgt, dass in der JVA Burg die Therapieakten getrennt von den Gefangenenpersonalakten geführt würden. Es gebe daher Akten, die sich auf die therapeutischen Maßnahmen beschränkten, um zu vermeiden, dass es zu datenschutzrechtlichen Verstößen käme. Im Rahmen einer Eingabe zur Führung der Gefangenenpersonalakte bei der JVA Burg stellte sich im Nachhinein heraus, dass diese getrennte Aktenführung bisher nur für die sozialtherapeutische Anstalt der JVA Halle gilt.

Der Landesbeauftragte hat in seinem Prüfbericht darauf hingewiesen, dass in Bayern auf der Rechtsgrundlage des Art. 201 BayStVollzG die Gefangenenpersonalakte getrennt von der Therapieakte geführt wird. Die Aufnahme einer solchen Regelung in das sachsen-anhaltische Recht wäre daher durchaus möglich und auch angemessen. Das Ministerium der Justiz hat eine entsprechende Prüfung zugesagt.

Herstellung und Verwendung von Verpflegungslisten

Im Rahmen einer Eingabe hatte ein Petent bemängelt – dies war auch Gegenstand der Beratung des Ausschusses für Recht und Verfassung des Landtages gewesen –, dass auf den von der Küche erstellten Verpflegungslisten für die Mittagsverpflegung in den Hafträumen Daten der behandelnden Ärzte sowie Angaben über besondere Kostformen in Verbindung mit Krankheitsdaten enthalten seien, die damit zur Kenntnis der privaten Dienstleister (und der anderen Gefangenen) gelangten. Nach einer Prüfung des Vorgangs hat das Ministerium der Justiz diesen rechtlich bedenklichen Zustand abgestellt. Die Gefangenen erhalten ihre Mittagskost jetzt in Assietten, die mit Akronymen versehen sind. Der Petitionsausschuss des Landtages, der mit dem Vorgang ebenfalls befasst war, wurde entsprechend unterrichtet. Von dem geänderten Verfahren hat sich der Landesbeauftragte vor Ort überzeugt.

Verwaltungshilfsdienste

Mitarbeiter der Firma Kötter leisten zudem Hilfsdienste bei der Führung der Gefangenenpersonalakte. Sie ordnen z. B. Unterlagen ein oder aus oder bereiten Wiedervorlagen vor. Diese Tätigkeit wird nicht überwacht. Im Rahmen dieser Hilfsdienstetätigkeit lässt es sich faktisch nicht vermeiden, dass der Mitarbeiter des privaten Dienstleisters Einsicht in die Gefangenenpersonalakten nimmt. Ebenso wirken beim Schreibdienst Mitarbeiter der Firma Kötter mit. Sofern Schreiben erstellt werden, die einfache Verwaltungsvorgänge der JVA Burg betreffen, wie z. B. fiskalische Hilfsgeschäfte, ist das unter daten-

schutzrechtlichen Gesichtspunkten nicht weiter problematisch. Die Mitarbeiter des privaten Dienstleisters bearbeiten jedoch auch Schreiben, die Gegenstand der Gefangenenpersonalakte sind. Sie erhalten auch so Einblick in sensible personenbezogene Daten der Gefangenen. Das Ministerium der Justiz hat in seiner Stellungnahme darauf verwiesen, dass die Mitarbeiter der privaten Dienstleister gem. § 155 StVollZG Einsicht in die Gefangenenpersonalakte nehmen dürften, da sie Verwaltungshelfer seien. § 155 StVollzG lässt jedoch nur den Einsatz von Verwaltungshelfern im Strafvollzug zu, trifft aber keine Aussage darüber, zu welcher konkreten Tätigkeit ein Verwaltungshelfer eingesetzt werden darf. Der Landesbeauftragte hat daher empfohlen, Mitarbeiter des privaten Dienstleisters zu Hilfsdiensten bei der Führung der Gefangenenpersonalakte nicht mehr heranzuziehen bzw. ihre Tätigkeit beim Schreibdienst auf weniger sensible Vorgänge zu beschränken.

Telefongespräche der Gefangenen

Die Benutzer des Gefangenen-Telefonsystems „Telio“ werden automatisch über eine Bandansage über die Möglichkeit des Abhörens des Gesprächs informiert. Die Ansage erfolgt daher auch dann, wenn das Gespräch nicht abgehört wird. Der Gesprächspartner wird damit auch in den Fällen über eine Inhaftierung des Gefangenen informiert, in denen dies – mangels Überwachung des Gesprächs – nicht notwendig gewesen wäre. Das Landgericht Stendal hat in einer noch nicht rechtskräftigen Entscheidung diese Praxis für rechtswidrig gehalten, da § 32 Sätze 3 und 4 StVollzG eine Benachrichtigung nur erforderlich machen, wenn die Überwachung auch erfolge. Die Auffassung des Ministeriums der Justiz, dass mit der bisherigen Praxis der Gesetzesvorgabe von § 32 Sätze 3 und 4 StVollzG entsprochen werde, steht somit im Widerspruch zur o. g. Entscheidung.

Feststellungen und Empfehlungen zur Datensicherheit

Bei den Empfehlungen des Landesbeauftragten zu den technischen und organisatorischen Maßnahmen zur Datensicherheit nach seinem Informations- und Kontrollbesuch in der JVA Burg kann von einer weitgehenden Umsetzung durch die JVA Burg, die IT-Leitstelle für den Justizvollzug Raßnitz bzw. das Ministerium der Justiz ausgegangen werden. Voraussetzung dafür ist allerdings, dass:

- die Ankündigungen und Zusagen des Ministeriums der Justiz, wie in seiner Antwort vom Februar 2011 auf den Prüfbericht des Landesbeauftragten gegeben, erfüllt werden und

- dem Landesbeauftragten ein aktueller Sachstand der Erarbeitung des neuen Datenschutzkonzepts der JVA Burg mitgeteilt wird.

Ausblick

Ob das zuletzt bis „spätestens“ Ende 2011 in Aussicht gestellte Datenschutzkonzept für die JVA Burg vorgelegt werden wird, erscheint aus Sicht des Landesbeauftragten fraglich.

In einigen Punkten besteht, wie bereits beschrieben, weiterhin erheblicher Erörterungsbedarf. Das betrifft insbesondere auch die Ergänzung des PPP-Vertragswerks um Regelungen der Auftragsdatenverarbeitung. So ist z. B. nicht nachvollziehbar, dass vom Ministerium der Justiz die Notwendigkeit einer Ergänzung des PPP-Vertragswerks um Regelungen der Auftragsdatenverarbeitung in Frage gestellt wird. Es ist offensichtlich, dass bei Abschluss der Verträge die Problematik der Auftragsdatenverarbeitung nicht gesehen wurde. Folglich können die Verträge keine ausreichenden Regelungen über die Auftragsdatenverarbeitung enthalten. Dementsprechend war schon ein Konsens darüber erzielt worden, dass das PPP-Vertragswerk im Vorgriff auf eine zukünftige Regelung im Strafvollzugsgesetz des Landes Sachsen-Anhalt durch ausdrückliche übergreifende Bestimmungen zur Auftragsdatenverarbeitung ergänzt werden sollte.

Sollte es in den kritischen Punkten nicht zu einer zufriedenstellenden Lösung kommen, behält sich der Landesbeauftragte eine Beanstandung der von ihm festgestellten Verstöße und Mängel gem. § 24 Abs. 1 DSG-LSA ausdrücklich vor. Er ist aber wie immer gesprächsbereit, um die noch ausstehenden Punkte einvernehmlich mit allen an diesem PPP-Projekt Beteiligten zu klären.

24.3 Kontrolle in einer JVA – Auftragsdatenverarbeitung in der Justiz

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 23.2) berichtet, dass er anlässlich einer Kontrolle einer Justizvollzugsanstalt festgestellt hatte, dass das Landgericht Magdeburg für die Justizvollzugsanstalt einen Vertrag zur Entsorgung von Datenträgern mit einem privaten Unternehmen geschlossen hatte. Es lag daher ein klassischer Fall der Auftragsdatenverarbeitung vor. Im Zuge der Nachforschungen stellte sich heraus, dass das Gericht entsprechende Verträge auch für eine weitere Justizvollzugsanstalt sowie für die in seinem örtlichen Zuständigkeitsbereich gelegenen Amtsgerichte und das Justizzentrum Magdeburg geschlossen hatte.

Der Landesbeauftragte hat das Justizministerium als für den Strafvollzug zuständige Fachaufsichtsbehörde um Auskunft gebeten, auf welcher Rechtsgrundlage das Gericht tätig geworden sei. Er hat das Ministerium darauf aufmerksam gemacht, dass der Auftrag nach § 8 Abs. 2 Sätze 1 und 2 DSG-LSA entweder durch die zuständige Stelle, in deren Auftrag die Daten verarbeiten werden sollen oder gem. § 8 Abs. 2 Satz 3 DSG-LSA durch die zuständige Fachaufsichtsbehörde erteilt werden müsse. Es sei nicht zweifelsfrei zu erkennen, dass das Handeln des Landgerichts Magdeburg den gesetzlichen Voraussetzungen entspreche, denn das Gericht sei weder die Stelle, in deren Auftrag die Daten hätten verarbeitet werden sollen, noch die für die Justizvollzugsanstalt zuständige Fachaufsichtsbehörde gewesen.

Erst nach mehrfachen Rückfragen zur einschlägigen Rechtsgrundlage hat das Justizministerium vorgetragen, dass das Landgericht Magdeburg zum Abschluss des Vertrags zur Entsorgung von Datenträgern für die o. g. Behörden und Gerichte berechtigt gewesen sei, da die Leiter der beteiligten Behörden die Präsidentin des Landgerichts Magdeburg zum Abschluss der Verträge ermächtigt hätten. Die Bevollmächtigung sei allerdings nicht schriftlich, sondern nur mündlich erfolgt. Die beteiligten Parteien seien daher gebe-

ten worden, die getroffenen Vereinbarungen auf eine schriftliche Basis zu heben.

Offensichtlich hat das Ministerium seine Argumentation für nicht ganz stichhaltig gehalten, denn es hat sich ferner darauf berufen, dass das Landgericht auch deshalb zum Abschluss der Verträge befugt gewesen sei, da ihm durch die Ausführungsvorschrift (AV) des Justizministeriums vom 3. Juli 1992 (MBl. LSA 1992 S. 928) die Aufgaben einer zentralen Beschaffungsstelle übertragen worden seien. Als solche sei das Gericht dann tätig geworden. Diese Auffassung ist jedoch nicht überzeugend. Die AV regelt allgemein die Zentralisierung des Beschaffungswesens für die Justizbehörden und bestimmt, nach welchen Vorschriften das Landgericht Magdeburg als zentrale Beschaffungsstelle Aufträge zu vergeben hat (§ 55 LHO nebst VV-LHO). Sie erfasst somit den Normalfall der Beschaffung von Bedarfsgütern. Dementsprechend geht sie auf die besonderen Anforderungen für Verträge, die Beschaffungen bzw. Entsorgungen im Rahmen einer Auftragsdatenverarbeitung betreffen, in ihrem Wortlaut nicht ein. So fehlt z. B. eine Bestimmung, aus der sich ergibt, dass das Ministerium der Justiz des Landes Sachsen-Anhalt das Recht nach § 8 Abs. 2 Satz 3 DSG-LSA als Fachaufsichtsbehörde, Verträge zur Auftragsdatenverarbeitung zu schließen, an das Landgericht Magdeburg delegiert hat.

Nicht geregelt ist auch der Umgang mit den sich aus § 8 Abs. 6 DSG-LSA ergebenden Prüfpflichten, die das Landgericht Magdeburg als Auftraggeber einzuhalten hätte. Im Übrigen ist darauf zu verweisen, dass die AV auch schon deshalb nicht als Rechtsgrundlage für den hier in Frage stehenden Abschluss von Entsorgungsverträgen herangezogen werden kann, weil sie die Entsorgung von Bedarfsgütern für die Justizbehörden gar nicht erfasst. Die Zuweisung von Aufgaben als Beschaffungsstelle für Sachgüter, z. B. Papier, ist ein Aliud gegenüber der Entsorgung von Datenträgern mit personenbezogenen Daten. Der Umstand, dass die AV nur kurze Zeit nach dem Inkrafttreten des DSG-LSA erlassen wurde und Regelungen zur Auftragsdatenverarbeitung in ihr nicht enthalten sind, spricht dafür, dass die Problematik bei ihrem Erlass nicht gesehen wurde.

Der Landesbeauftragte hat daher das Justizministerium gebeten, seine Rechtsauffassung zu überprüfen. In seiner Stellungnahme hat das Ministerium dem Landesbeauftragten mitgeteilt, dass es sich bei der Berufung auf die AV lediglich um eine Hilfserwägung gehandelt habe, es solle bei der Lösung der Einzelbevollmächtigung bleiben.

Unter datenschutzrechtlichen Gesichtspunkten ist das gewählte Konstrukt nicht optimal, da das Landgericht Magdeburg für die von ihm vertretenen Behörden und Gerichte zwar die Verträge über die Auftragsdatenverarbeitung schließt, später aber für die Überwachung der Einhaltung der von ihm ausgehandelten Regelungen nicht mehr zuständig ist; denn dies ist nach § 8 DSG-LSA die Aufgabe der Stelle, in deren Auftrag die Daten erhoben, verarbeitet oder genutzt werden. Die Kontrolle des Auftragnehmers ist also Aufgabe der vertretenen Stelle. Unter datenschutzrechtlichen Aspekten wäre es vorzugswürdig, wenn Vertragsabschluss und Kontrolle in einer Hand lägen. Da davon auszugehen ist, dass bei den vertretenen Stellen hinreichender juristischer Sachverstand zum Abschluss von Verträgen zur Auftragsdatenver-

arbeitung vorhanden ist, stellt sich ohnehin die Frage, ob es überhaupt der Einschaltung eines Vertreters bedarf.

24.4 Elektronische Fußfessel

Mit seinem Urteil vom 17. Dezember 2009 (NJW 2010, 2495) hatte der Europäische Gerichtshof für Menschenrechte (EGMR) die nachträgliche Sicherungsverwahrung für unvereinbar mit der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) erklärt, da sie als eine dem strikten Rückwirkungsverbot des Artikels 7 Abs. 1 Satz 2 EMRK unterliegende Strafe anzusehen sei. Mit dem „Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung und zu begleitenden Regelungen“ vom 22. Dezember 2010 (BGBl. I 2010 S. 2300) hat der deutsche Gesetzgeber u. a. die anfängliche Sicherungsverwahrung konsolidiert und die Möglichkeiten zur Anordnung einer nachträglichen Sicherungsverwahrung beschränkt. Gleichzeitig hat er für diejenigen Fälle, in denen eine nachträgliche Sicherungsverwahrung nach der Rechtsprechung des EGMR nicht mehr möglich war, ein Gesetz zur Therapierung und Unterbringung psychisch gestörter Gewalttäter (ThUG) erlassen (BGBl. I 2010 S. 2305).
Zum Entwurf des Landesausführungsgesetzes zum ThUG beteiligte die Landesregierung den Landesbeauftragten wie auch andere betroffene Institutionen nicht. Bei einer Anhörung im Landtag zum Gesetzentwurf (LT-Drs. 6/36) monierte der Landesbeauftragte die inkohärente Anwendung von Datenverarbeitungsregelungen des Maßregelvollzugsgesetzes. Die ganze Rechtsmaterie steht auf wackligen Beinen. Das Gesetz trat am 23. Juli 2011 in Kraft (GVBl. LSA 2011 S. 620).

Im Zuge der Neuregelung hat der Bundesgesetzgeber im Rahmen der Führungsaufsicht die Möglichkeit einer neuen strafbewehrten und von der Einwilligung des Verurteilten unabhängigen Weisung geschaffen, mit der einer verurteilten Person aufgegeben werden kann, die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen, vgl. § 68b Absatz 1 Satz 1 Nr. 12 StGB. Es handelt sich um die sog. elektronische Fußfessel, die in der Politik auch als Alternative für die Sicherheitsverwahrung oder für Ersatzfreiheitsstrafen, die für Geldstrafen verhängt wurden, diskutiert wurde.

Die Regelungen der elektronischen Fußfessel, die am 1. Januar 2011 in Kraft getreten sind, sollen nach der Vorstellung des Gesetzgebers vor allem spezialpräventiv wirken, da sie eine bessere Überwachung der Einhaltung von aufenthaltsbezogenen Weisungen ermöglichen und somit ein erhöhtes Entdeckungsrisiko im Falle einer erneuten schweren Straftat begründen sollen. Zudem soll es den Behörden erleichtert werden, im Falle einer von dem Straftäter ausgehenden gegenwärtigen erheblichen Gefahr für Leib oder Leben einzuschreiten (BT-Drs. 17/3403).

Voraussetzung für die richterliche Anordnung der elektronischen Aufenthaltsüberwachung ist, dass

- die Führungsaufsicht aufgrund der vollständigen Vollstreckung einer Freiheitsstrafe oder Gesamtfreiheitsstrafe von mindestens drei Jahren oder auf Grund einer erledigten Maßregel eingetreten ist,

- die Freiheitsstrafe oder Gesamtfreiheitsstrafe oder die Unterbringung wegen einer schweren Straftat i. S. d. § 66 Abs. 3 Satz 1 StGB (z. B. bestimmte Sexualstraftaten gegen Kinder, Jugendliche oder widerstandsunfähige Personen) verhängt oder angeordnet wurde,

- die Gefahr besteht, dass die verurteilte Person weitere derartige Straftaten begehen wird, und

- die Weisung erforderlich erscheint, um die verurteilte Person von der Begehung weiterer derartiger Straftaten abzuhalten.

Damit der Aufenthalt überwacht werden kann, müssen notwendigerweise die Aufenthaltsdaten erhoben, an die Aufsichtsstelle übermittelt und von dieser verwendet werden dürfen. Daher bestimmt ein neuer Absatz 4 in § 463a StPO, in welchem konkreten Umfang dies zulässig ist. Dabei sollen eine enge Zweckbindung, eine relativ kurze Speicherfrist und der Umstand, dass die Wohnung des Betroffenen erhebungsfreier Raum ist, wesentliche Sicherungen dafür sein, dass der Eingriff in das Grundrecht auf informationelle Selbstbestimmung verhältnismäßig bleibt.

In seinem Urteil vom 4. Mai 2011 (NJW 2011, 1931) hat das Bundesverfassungsgericht mittlerweile entschieden, dass alle Vorschriften über die Anordnung und Dauer der Sicherungsverwahrung mit dem Freiheitsgrundrecht des Untergebrachten nicht vereinbar sind, weil sie den Anforderungen des verfassungsrechtlichen Gebots eines deutlichen Abstands des Freiheitsentzugs vom Strafvollzug (sog. Abstandsgebot) nicht genügen. Überdies verletzen die Vorschriften zur nachträglichen Verlängerung der Sicherungsverwahrung über die frühere Zehnjahresfrist hinaus und zur nachträglichen Anordnung der Sicherungsverwahrung das rechtsstaatliche Vertrauensschutzgebot aus Art. 2 Abs. 2 Satz 2 i. V. m. Art. 20 Abs. 3 GG. Die Sicherungsverwahrung muss folglich erneut überarbeitet werden, sie darf keine verlängerte Haft sein. Die elektronische Fußfessel war von dem Urteil dagegen nicht betroffen. Eine Klage gegen letztere ist vor dem Bundesverfassungsgericht jedoch anhängig.

Die für den Strafvollzug zuständigen Länder stehen indessen unter einem hohen Zeitdruck, da sie die gesetzlichen Voraussetzungen für den Einsatz der Fußfesseln schaffen müssen, und die Gerichte die elektronische Aufenthaltsüberwachung bereits anordnen können. Nennenswerte praktische Erfahrungen besitzt jedoch nur Hessen, in dem die elektronische Fußfessel aufgrund eines Pilotprojekts bereits zum Einsatz gekommen ist.

Vor diesem Hintergrund haben Hessen und Bayern als Vorreiter für die übrigen Bundesländer Ende Mai 2011 den gemeinsamen Betrieb und die Nutzung eines Systems der elektronischen Aufenthaltsüberwachung im Wege einer Verwaltungsvereinbarung geregelt und einen Staatsvertrag unterzeichnet, der die Einrichtung einer Gemeinsamen elektronischen Überwachungsstelle der Länder (GÜL) mit Sitz im hessischen Bad Vilbel zum Gegenstand

hat. Das Projekt wurde den Datenschutzbeauftragten des Bundes und der Länder auf dem Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragen des Bundes und der Länder im Mai 2011 vorgestellt. Folgendes Verfahren ist vorgesehen:

Zunächst wird im Rahmen einer Fallkonferenz entschieden, welche Personen (Probanden) die rechtlichen Voraussetzungen für die Anordnung einer elektronischen Aufenthaltsüberwachung erfüllen. Die Prüfung soll dabei so frühzeitig erfolgen, dass die Anlegung des Überwachungsgerätes noch vor der Entlassung des Probanden durchgeführt werden kann. Nach erfolgter Anlegung der elektronischen Fußfessel werden die Standortdaten an die Hessische Zentrale für Datenverarbeitung (HZD) übermittelt, die die Daten speichert und mit den ortsbezogenen Daten der richterlich angeordneten Gebots- und Verbotszonen vergleicht. Im Falle eines möglichen Verstoßes übermittelt die HZD die Daten an die GÜL, die wiederum Kontakt mit dem Probanden aufnimmt, um zu klären, ob tatsächlich ein Verstoß vorliegt. Ist das der Fall, wendet sich die GÜL an eine Kontaktstelle der Polizei des Landes, die nun die örtlich zuständige Polizeidienststelle einschaltet, damit diese für die Einhaltung der Weisung sorgen kann. Ferner wird die Führungsaufsicht von dem Verstoß informiert.

Für die Datenverarbeitung wird hessisches Recht gelten. Der hessische Landesbeauftragte für den Datenschutz wird für die Kontrolle der Einhaltung des Datenschutzrechts zuständig sein. Der Arbeitskreis stellte allerdings fest, dass noch einige datenschutzrechtliche Problemkreise offen sind. So soll z. B. das Anlegen der Überwachungsgeräte durch einen privaten Dienstleister erfolgen. Noch nicht abschließend geklärt ist auch die Frage, ob die Polizei die übermittelten Daten aufgrund des Polizeirechts nutzen darf oder hierzu eine spezialgesetzliche Rechtsgrundlage geschaffen werden muss.

Mittlerweile zeichnet sich ab, dass alle Bundesländer, also auch Sachsen-Anhalt, dem Staatsvertrag beitreten wollen. Es ist auch hier nachdrücklich zu kritisieren, dass der Landesbeauftragte von dem zuständigen Ministerium der Justiz bisher nicht über das Vorhaben unterrichtet wurde.

25 Telekommunikations- und Medienrecht

25.1 Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat am 2. März 2010 das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (s. Nr. 20.3) für verfassungswidrig und zugleich für nichtig erklärt (NJW 2010, 833). Das Gesetz verpflichtete Anbieter öffentlich zugänglicher Telefondienste sowie Anbieter von E-Mail- und Internetzugangsdiensten, umfangreiche Verkehrsdaten für sechs Monate auf Vorrat für die Strafverfolgungsbehörden zu speichern, ohne dass ein konkreter Verdacht vorliegt (s. IX. Tätigkeitsbericht, Nr. 24.1).

Der Erste Senat des Bundesverfassungsgerichts begründete seine Entscheidung damit, dass diese Datensammlung gegen Art. 10 Abs. 1 GG verstoße. Zwar sei eine Speicherungspflicht in dem vorgesehenen Umfang nicht von

vornherein verfassungswidrig. Es fehle aber insbesondere im Hinblick auf die immense Streubreite an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Erforderlich sind danach hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes. Das Bundesverfassungsgericht ordnete deshalb in seiner Entscheidung an, dass alle seit Erlass des Gesetzes erhobenen Daten unverzüglich zu löschen seien.

Unter einer Reihe enger Vorgaben könnte eine Vorratsdatenspeicherung nach Auffassung des Bundesverfassungsgerichts allerdings möglich sein. Hierzu gehören unter anderem die Gewährleistung eines besonders hohen Standards der Datensicherheit sowie das Vorliegen von schwerwiegenden Straftaten.

Nach dem Urteil obliegen dem Bundesgesetzgeber gem. Art. 73 Abs. 1 Nr. 7 GG die Gewährleistung der Datensicherheit sowie die normenklare Begrenzung der Zwecke der möglichen Datenverwendung als untrennbare Bestandteile der Anordnung der Speicherungsverpflichtung. Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben und die sich am Stand der Technik orientieren.

Der Abruf und die unmittelbare Nutzung der Daten sind nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürfen sie nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.

Eine nur mittelbare Nutzung der Daten zur Erteilung von Auskünften durch die Telekommunikationsdiensteanbieter über die Inhaber von IP-Adressen ist auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten können solche Auskünfte nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden.

Aus Sicht des Datenschutzes wäre es wünschenswert gewesen, wenn das Bundesverfassungsgericht die anlasslose Speicherung von Verkehrsdaten auf Vorrat gänzlich für verfassungswidrig erklärt hätte. Deshalb haben sich die Datenschutzbeauftragten des Bundes und der Länder nach dem Urteil des Bundesverfassungsgerichts in einer Entschließung (**Anlage 9**) erneut gegen die Vorratsdatenspeicherung ausgesprochen und die Bundesregierung aufgefordert, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Die Richtlinie 2006/24/EG war Gegenstand einer Evaluierung durch die Europäische Kommission, in deren Rahmen die Vereinbarkeit mit der Grundrechte-Charta zu kurz kam. Drei Mitgliedstaaten „verstoßen“ gegen die Richt-

linie, obwohl ihre Umsetzungsmaßnahmen von ihren jeweiligen Verfassungsgerichten für nichtig erklärt wurden. In zwei weiteren Mitgliedstaaten steht die Umsetzung noch aus. Die Kommission hat im Anschluss an den Bericht vom April 2010 mit einer Konsultation und Folgenabschätzung begonnen.

Eine wesentliche Aussage im Urteil des Bundesverfassungsgerichts besteht darin, dass zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehöre, die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total zu erfassen und zu registrieren. Hierfür habe sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen (vgl. Nr. 1). Es ist daher widersinnig, eine Vorratsdatenspeicherung noch vor Abschluss des europäischen Abstimmungsprozesses wieder einzuführen. Kritisch sind auch andere Vorhaben, die eine Vorratsdatenspeicherung zum Ziel haben, zu betrachten. Das gilt z. B. für den elektronischen Entgeltnachweis (vgl. Nr. 22.10).

Auch nach der Evaluierung und einer entsprechenden Novellierung der Richtlinie wäre es fraglich, ob eine Umsetzung in nationales Recht unter den strengen Vorgaben des Bundesverfassungsgerichtsurteils möglich ist.

Anfang des Jahres 2011 hat die Bundesjustizministerin ein „Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“ vorgelegt. In dem darin vorgeschlagenen grundrechtsschonenden Quick-Freeze-Verfahren kann nur die Sicherung von Verkehrsdaten solcher Personen angeordnet werden, die einen hinreichenden Anlass dazu gegeben haben. Die bei den Telekommunikationsunternehmen aus geschäftlichen Gründen bereits vorhandenen Verkehrsdaten sollen also anlassbezogen gesichert ("eingefroren") werden und so den Ermittlern unter Richtervorbehalt eine begrenzte Zeit zur Verfügung stehen können. Im Internetbereich soll eine auf sieben Tage befristete Speicherung von Verkehrsdaten erfolgen, um bei einem konkreten Verdacht dynamische IP-Adressen Personen zuordnen zu können (vgl. auch BGH, Urteil vom 13. Januar 2011, NJW 2011, 1509). Seit dem Frühsommer 2011 liegt auch ein entsprechender Gesetzentwurf vor; die rechtspolitische Diskussion dauert an.

25.2 Neuregelung der Rundfunkfinanzierung

Am 15. Dezember 2010 haben die Ministerpräsidenten der Länder den 15. Rundfunkänderungsstaatsvertrag unterzeichnet und damit eine Reform der Finanzierung für den öffentlich-rechtlichen Rundfunk beschlossen. Zukünftig wird die an das Vorhandensein eines Empfangsgerätes gebundene Rundfunkgebühr durch einen Rundfunkbeitrag ersetzt, der für jeden Haushalt und, gestaffelt nach Anzahl der Beschäftigten, für jede Betriebsstätte zu entrichten ist.

Der auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderte Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks hätte die Möglichkeit eröffnen können, die Befugnisse zur Erhebung und Speicherung personenbezogener Daten bei den Landesrundfunkanstalten bzw. der Gebühreneinzugszentrale (GEZ) einzuschränken

und damit eine datenschutzgerechte Beitragserhebung umzusetzen. Diese Erwartung hat sich leider nicht erfüllt.

Aus datenschutzrechtlicher Sicht wurde den Grundsätzen der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nicht ausreichend Rechnung getragen. Wesentlicher Kritikpunkt sind die umfangreichen Datenerhebungsbefugnisse der Landesrundfunkanstalten, wobei die Erhebung ohne Kenntnis des Betroffenen bei öffentlichen und nichtöffentlichen Stellen erfolgen kann. Damit besteht auch die Möglichkeit, Daten von Adresshändlern anzukaufen. Dies wurde bereits in der Vergangenheit von den Datenschutzbeauftragten des Bundes und der Länder als unverhältnismäßig abgelehnt (s. VII. Tätigkeitsbericht, Nr. 23.5).

Ein weiterer Kritikpunkt ist die Übermittlung von Daten aller volljährigen Personen durch die Meldeämter zusätzlich zu den in den Landesmeldegesetzen bereits enthaltenen Meldedatenübermittlungsbefugnissen. Außerdem ist vorgesehen, dass bei einem Antrag auf Befreiung von der Beitragspflicht bzw. auf Ermäßigung des Rundfunkbeitrages weiterhin neben einer Bescheinigung auch die Originalbescheide oder beglaubigte Kopien dieser Bescheide vorgelegt werden können. Durch das Einscannen der Bescheide werden eine Vielzahl nicht erforderlicher sensibler personenbezogener Daten erhoben und verarbeitet.

Zu den vorgelegten Entwürfen des Staatsvertrages haben die Datenschutzbeauftragten des Bundes und der Länder umfassend Stellung genommen. In einer Anhörung, die am 11. Oktober 2010 in Berlin stattfand, wurde ebenfalls auf die datenschutzrechtlich kritischen Punkte hingewiesen. Zeitgleich wurde eine Entschließung verabschiedet, die die wesentlichen Forderungen der Datenschutzbeauftragten des Bundes und der Länder enthält (**Anlage 15**).

Vor Abschluss des 15. Rundfunkänderungsstaatsvertrages fand am 26. November 2010 auch im Landtag von Sachsen-Anhalt eine Anhörung statt, zu der der Landesbeauftragte eingeladen wurde und bei der nochmals Gelegenheit bestand, die Kritikpunkte darzulegen.

Im Ergebnis blieben viele datenschutzrechtliche Forderungen unberücksichtigt. So wird bei Anträgen auf Beitragsbefreiung oder -ermäßigung auch weiterhin nicht auf die Vorlage des vollständigen Leistungsbescheides verzichtet. Allerdings wurde die Regelung hinsichtlich der Datenerhebung bei Adresshändlern in den Übergangsvorschriften bis zum 31. Dezember 2014 ausgesetzt, d. h. bis zu diesem Zeitpunkt dürfen die Landesrundfunkanstalten keine Adressdaten privater Personen ankaufen. Außerdem wird der einmalige Meldedatenabgleich nicht innerhalb von zwei Jahren ab Inkrafttreten des Staatsvertrages, sondern an einem bundeseinheitlichen Stichtag erfolgen.

Der 15. Rundfunkänderungsstaatsvertrag wird am 1. Januar 2013 in Kraft treten, wenn bis spätestens zum 31. Dezember 2011 eine Ratifizierung durch die Länderparlamente erfolgt ist (vgl. für Sachsen-Anhalt LT-Drs. 6/165). Ansonsten wird der Staatsvertrag, wie beim 14. Rundfunkänderungsstaatsvertrag geschehen (s. Nr. 25.7), gegenstandslos.

25.3 Sperrung von Internetseiten zur Bekämpfung von Kinderpornographie

Bereits in seinem letzten Tätigkeitsbericht (Nr. 24.5) hatte sich der Landesbeauftragte zu dem am 18. Juni 2009 vom Bundestag beschlossenen Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz) geäußert. Das Gesetz sah vor, den Zugriff auf kinderpornographische Seiten im Internet zu sperren. Mit Hilfe einer vom Bundeskriminalamt geführten Sperrliste sollten die Provider den Zugriff auf die in der Liste enthaltenen Webseiten über DNS-Sperren verhindern.

Das Gesetz wurde u. a. von der Fachpresse, von Juristen, Bürgerrechtlern, aber auch von Missbrauchsopfern kritisiert. 134.000 Menschen unterzeichneten eine Onlinepetition gegen die Internetsperren. Die starke öffentliche Kritik begründet sich darin, dass durch die Sperren Kinderpornographie nicht bekämpft, aber u. U. ein Instrument zur allgemeinen Zensur im Internet geschaffen werden könnte.

Im Rahmen der Koalitionsverhandlungen 2009 beschlossen CDU/CSU und FDP, die Internetsperren zunächst auszusetzen und stattdessen eine Löschung der kinderpornographischen Inhalte anzustreben. Der damalige Bundespräsident Horst Köhler bat die Bundesregierung vor der Entscheidung darüber, ob er das Gesetz unterzeichnet oder nicht, um ergänzende Informationen. Am 17. Februar 2010 unterzeichnete der Bundespräsident das Gesetz, da keine durchgreifenden verfassungsrechtlichen Bedenken bestanden hätten. Am 22. Februar 2010 wurde das Gesetz im Bundesgesetzblatt veröffentlicht (BGBl. I S. 78) und trat am 23. Februar in Kraft. Das Bundeskriminalamt wurde daraufhin vom Bundesministerium des Innern durch einen Erlass angewiesen, dennoch keine Sperrliste zu erstellen.

Seine Erfolge beim Löschen von kinderpornographischen Inhalten im Internet hat das Bundeskriminalamt bereits evaluiert und im Januar 2011 festgestellt, dass in 97 von 143 Fällen (68 Prozent) die kinderpornographischen Inhalte innerhalb einer Woche gelöscht waren. Nach zwei Wochen lag die Quote bereits bei 93 Prozent und stieg nach drei Wochen auf 98 Prozent an. Nach vier Wochen waren die Daten in 142 von 143 Fällen (99 Prozent) gelöscht. Anhand dieser Zahlen ist erkennbar, dass der Ansatz „Löschen statt Sperren“ im Kampf gegen kinderpornographische Inhalte im Internet erfolgreich ist.

Die am 13. April 2011 vom Bundeskabinett beschlossenen Eckpunkte für ein Gesetz zur Umsetzung des Grundsatzes „Löschen statt Sperren“ sehen die Aufhebung des Artikels 1 des Zugangserschwerungsgesetzes vor. Kinderpornographische Inhalte werden auch weiterhin auf der Grundlage des geltenden Rechts gelöscht. Die Befugnis des Telekommunikationsanbieters zur Erhebung von Daten nach § 96 TKG wird als Folgeänderung aus dem TKG gestrichen, soweit sie sich auf das Sperren nach dem Zugangserschwerungsgesetz bezieht. Auch die in Artikel 3 des Zugangserschwerungsgesetzes geregelte Evaluierungs- und Berichterstattungspflicht wird aufgehoben, da mit dem Verzicht auf das Sperren auch der Evaluierungsgegenstand entfällt. Der Gesetzentwurf liegt in BR-Drs. 319/11 vor.

Schien das Thema Websperren damit endgültig vom Tisch zu sein, wurde es in einem anderen Bereich als vermeintliche Lösung wieder aufgewärmt: Der Entwurf einer Novellierung des Glücksspielstaatsvertrages vom Frühjahr 2011 sieht Sperrverfügungen gegen Provider zwecks Verhinderung illegaler, nicht-lizensierter Glücksspielanbieter vor, unter Inkaufnahme von Einschränkungen des Fernmeldegeheimnisses. In einer Anhörung der Länder in Magdeburg kritisierte der Landesbeauftragte für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dies ebenso wie die fehlende Normenklarheit dieser und anderer Vorschriften. Das Thema Websperren will die Ministerpräsidentenkonferenz offenbar nicht weiterverfolgen.

25.4 Musterdienstanweisung zur Nutzung von E-Mail und Internet am Arbeitsplatz

Die im Jahr 2001 vom Ministerium des Innern herausgegebene Musterdienstanweisung über die Bereitstellung und Nutzung von Internet-Zugängen war aufgrund der seit Ende 2005 im damaligen Landesinformationszentrum durchgeführten zentralen Spamfilterung (s. Nr. 25.5) zu überarbeiten. In diesem Zusammenhang hatte der Landesbeauftragte empfohlen, die ausnahmsweise private Nutzung des Internets weiterhin zu gestatten, die private E-Mail-Kommunikation aber nur mittels Web-Mail zu erlauben, d. h. die private Nutzung der dienstlichen E-Mail-Adresse zu untersagen. Dieser Empfehlung ist die Staatssekretärskonferenz leider nicht gefolgt.

Bereits in seinem VIII. Tätigkeitsbericht (Nr. 23.5) und IX. Tätigkeitsbericht (Nr. 24.6) hatte sich der Landesbeauftragte zu Problemen bei der erlaubten privaten Nutzung der dienstlichen E-Mail-Adresse geäußert.

Die zum Redaktionsschluss des letzten Tätigkeitsberichts noch immer nicht vorliegende geänderte Fassung der Musterdienstanweisung wurde dem Landesbeauftragten erst im Juni 2010 zur Kenntnis gegeben. Zuvor war sie an die Ressorts mit dem Hinweis verteilt worden, dass es sich hierbei um ein Muster handelt, von welchem abgewichen werden kann und dessen Umsetzung in eigener Verantwortung vorzunehmen ist.

Die geänderte Musterdienstanweisung enthält nunmehr den Hinweis, den ausnahmsweisen privaten E-Mail-Verkehr möglichst über Web-Maildienste abzuwickeln. Für die private Internet- und E-Mail-Nutzung muss der Bedienstete darin einwilligen, dass auch die private Nutzung protokolliert und stichprobenhaft kontrolliert wird, dass eine Spamfilterung aller eingehenden E-Mails erfolgt und dass im Einzelfall eine Einsichtnahme in private E-Mails erfolgen kann. Außerdem ist der Bedienstete verpflichtet, seine privaten Kommunikationspartner darauf hinzuweisen, dass es sich um ein dienstliches E-Mail-Postfach handelt und eine Protokollierung sowie stichprobenhafte Kontrolle durchgeführt werden.

Der Landesbeauftragte wird auch in Zukunft im Rahmen seiner Beratungstätigkeit den öffentlichen Stellen empfehlen, rechtssichere, transparente Regelungen zu schaffen.

25.5 Spamfilterung von E-Mails im Landesnetz

In ihrer Stellungnahme zu Nr. 24.7 des IX. Tätigkeitsberichts informierte die Landesregierung, dass auf Grundlage der Studie „Antispam-Strategien, Unerwünschte E-Mails erkennen und abwehren" des Bundesamtes für Sicherheit in der Informationstechnik die durch das damalige Landesinformationszentrum als IT-Dienstleister realisierte Antispam-Strategie des Landes Sachsen-Anhalt überprüft worden ist.

In der Vergangenheit wurden als Spam klassifizierte E-Mails sowie E-Mails mit unzulässigen Dateianhängen (unzulässiges Dateiformat, zu langer Dateiname) in einem sogenannten Quarantäneverzeichnis gespeichert und nach 30 Tagen gelöscht. Dabei wurden nur Empfänger von E-Mails mit unzulässigen Dateianhängen darüber informiert, dass ihre E-Mail im Quarantäneverzeichnis zwischengespeichert wurde.

Um ein für alle Nutzer transparentes Verfahren einzuführen, das auch dem bei ausnahmsweise privater Nutzung der dienstlichen E-Mail-Adresse (s. Nr. 25.4) zu beachtenden Fernmeldegeheimnis Rechnung trägt, werden die Spam-Mails nicht mehr zwischengespeichert, sondern als Spam markiert und an die Empfänger weitergeleitet. Vorher ist es jedoch erforderlich, das Spam-Aufkommen und damit die Menge weitergeleiteter E-Mails erheblich zu reduzieren.

Dazu erfolgt am E-Mail-Gateway des Landes zunächst ein Greylisting. Anschließend wird die Gültigkeit der Empfänger anhand des zentralen Adressverzeichnisdienstes geprüft (sog. Recipient Check). Alle aufgrund unbekannter Empfänger nicht zustellbaren E-Mails werden abgewiesen. Danach werden die E-Mails einer Spamfilterung unterzogen, von einem Virenscanner geprüft und – ggf. mit Spam-Markierung – an die Postfachserver der jeweiligen Ressorts weitergeleitet. Für die Pflege der Adresseinträge im zentralen Adressverzeichnisdienst und den Umgang mit den markierten E-Mails ist das jeweilige Ressort zuständig.

Zum 1. Februar 2010 wurde die Spamquarantäne im Landesrechenzentrum, welches als zentraler IT-Dienstleister für die Landesverwaltung am 1. September 2009 aus dem Landesinformationszentrum und dem Finanzrechenzentrum gebildet wurde, endgültig abgeschaltet, da der überwiegende Teil der Behörden durch den Recipient Check erfasst wird.

25.6 EU-Parlament beschließt „Telekom-Paket“

Das Richtlinienpaket zur Novellierung des Regulierungsrahmens für Telekommunikationsnetze, das sogenannte „Telekom-Paket“, trat am 19. Dezember 2009 in Kraft. Das Reformpaket umfasst die Richtlinie 2009/140/EG zur Änderung der Rahmenrichtlinie (RRL), der Zugangsrichtlinie und der Genehmigungsrichtlinie, die Richtlinie 2009/136/EG zur Änderung der Universaldienstrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation (die sogenannte E-Privacy-Richtlinie) sowie die Verordnung (EG) Nr. 1211/2009 zur Errichtung des neuen Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK).

Die Verabschiedung des Pakets verzögerte sich, da die Frage der Sperrung des Internetzugangs bei Urheberrechtsverletzungen bis zum Schluss stark umstritten blieb. Mit den Bestimmungen in Art. 1 Abs. 3a RRL wurde ein Kompromiss gefunden, der das Scheitern der Reform verhinderte. Dort wird festgelegt, dass die Mitgliedstaaten bei jeglichen Maßnahmen, die sie in Bezug auf den Zugang und die Nutzung von Diensten und Anwendungen über elektronische Kommunikationsnetze ergreifen, die Grundrechte und Grundfreiheiten der Bürger beachten müssen. Außerdem müssen diese Maßnahmen angemessen, verhältnismäßig und notwendig sein. Dabei haben die Bürger Anspruch auf ein faires und unparteiisches Verfahren sowie auf eine effektive und rechtzeitige gerichtliche Überprüfung.

Ein wichtiger Bestandteil des neuen Rechtsrahmens ist die Reform der Richtlinie über den Datenschutz in der elektronischen Kommunikation. Diensteanbieter werden u. a. verpflichtet, die personenbezogenen Daten ihrer Kunden vor unbeabsichtigter Zerstörung und Verlust sowie unbefugtem Zugang bzw. unbefugter Weitergabe zu bewahren. Im Fall einer Verletzung des Schutzes personenbezogener Daten müssen die Diensteanbieter die zuständige Behörde und u. U. auch den betroffenen Kunden über die Datenpanne informieren.

Des Weiteren enthält die E-Privacy-Richtlinie eine Regelung, die die datenschutzrechtlichen Voraussetzungen beim Umgang mit Cookies neu festlegt. Die bisherige Widerspruchslösung (Opt-Out) wird durch eine Einwilligungslösung (Opt-In) mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt.

Bezüglich der Verbraucherrechte gilt künftig, dass für das automatisierte Versenden von Reklamebotschaften per E-Mail, Fax, SMS oder MMS sowie für maschinelle Marketinganrufe eine vorherige Zustimmung der Kunden einholt werden muss. Dazu kommt der Anspruch auf einen Anbieterwechsel innerhalb eines Arbeitstages mit Beibehaltung der bisherigen Telefonnummer sowie die Begrenzung maximaler Vertragslaufzeiten auf zwei Jahre.

Obwohl die neuen Bestimmungen von den Mitgliedsstaaten innerhalb von 18 Monaten, d. h. bis zum 25. Mai 2011, in nationales Recht umgesetzt werden müssen, hat das Bundeskabinett erst am 2. März 2011 einen Entwurf zur Novellierung des Telekommunikationsgesetzes beschlossen (BR-Drs. 129/11). Geplant ist die Einführung einer Informationspflicht gegenüber der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie u. U. auch gegenüber den Betroffenen bei einer Verletzung des Schutzes personenbezogener Daten. Die Informationspflicht über sogenannte Datenpannen soll für Anbieter öffentlich zugänglicher Telekommunikationsdienste gelten. Diese Anbieter müssen auch ein Verzeichnis über solche Verletzungen führen.

Mit einer Änderung des Telemediengesetzes hinsichtlich der o. g. Cookie-Regelung war zunächst nicht zu rechnen, da Einzelfragen der Umsetzung Gegenstand umfangreicher Konsultationen auf europäischer Ebene sind. Bereits im November 2010 wurde vom zuständigen Bundesministerium für Wirtschaft und Technologie mitgeteilt, dass eine Änderung nicht für notwendig erachtet werde, da der geltende Telemediendatenschutz in seiner grundsätz-

lichen Ausrichtung auch der nunmehr strengeren Regelung entspreche. Aus diesem Grund haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 24./25. November 2010 einen Beschluss gefasst, der die Änderung der Widerspruchslösung fordert (**Anlage 26**). Der Bundesrat griff dies in einer Gesetzesinitiative vom 17. Juni 2011 auf (BR-Drs. 156/11).

25.7 Jugendmedienschutz-Staatsvertrag

Im Rahmen des 14. Rundfunkänderungsstaatsvertrages beschlossen die Ministerpräsidenten der Länder am 10. Juni 2010 eine Novellierung des Jugendmedienschutz-Staatsvertrages (JMStV). Die Änderungen, die nach Ratifizierung durch die Landesparlamente (vgl. GVBl. LSA S. 546) am 1. Januar 2011 in Kraft treten sollten, wurden kontrovers diskutiert. Kernpunkt war die geplante Einführung einer Alterskennzeichnung für Inhalte im Internet.

Kritiker bemängelten, dass ein untauglicher Versuch unternommen würde, die etablierten Regeln für Film und Fernsehen auf das Internet zu übertragen. Dies sei unpraktikabel und würde Rechtsunsicherheit schaffen, da bei einer versehentlich fehlerhaften Kennzeichnung nach Ansicht vieler Juristen mit einer Abmahnwelle von Mitbewerbern oder Verbänden in ganz erheblichem Umfang zu rechnen sei.

Die Befürworter sahen dagegen in der Alterskennzeichnung eine Stärkung des Selbstregulierungsprinzips und einen praktikableren Mechanismus als Sendezeitbeschränkungen und Jugendschutzprogramme, wie sie auch im derzeit geltenden JMStV bei entwicklungsbeeinträchtigenden Angeboten gefordert werden (vgl. § 5 Abs. 3 i. V. m. § 11 JMStV).

Der nordrhein-westfälische Landtag sprach sich am 16. Dezember 2010 einstimmig gegen den 14. Rundfunkänderungsstaatsvertrag und damit gegen die Novellierung des JMStV aus. Damit ist die Änderung nicht in Kraft getreten. Bis zur Neuregelung bleibt der seit 2003 bestehende JMStV in Kraft.

25.8 Granada-Charta

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation hat auf ihrer 47. Sitzung am 15./16. April 2010 in Granada eine „Charta zur Regelung der Datennutzung in der digitalen Welt“ verabschiedet (http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2010/34_GranadaCharta.html).

Die Charta, die auf eine Initiative des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zurückgeht, stellt in insgesamt 20 Grundsätzen Regeln für den verantwortlichen Umgang mit Daten im digitalen Umfeld auf. Sie richtet sich sowohl an Nutzer als auch an Anbieter von Telekommunikationsdiensten und Telemedien sowie an öffentliche Stellen.

Die Nutzer sollten sich immer bewusst sein, welche Konsequenzen sich durch die Veröffentlichung personenbezogener Daten im Internet ergeben, da eine Löschung der Daten oft nicht oder nur schwer möglich ist.

Die Anbieter von Telekommunikationsdiensten und Telemedien sollten ihre Angebote so ausgestalten, dass eine datenschutzkonforme Nutzung möglich ist. Sie sollten angemessene technisch-organisatorische Maßnahmen zur Wahrung der Sicherheit ihrer Dienste treffen und den korrekten Umgang mit ihnen anvertrauten personenbezogenen Daten garantieren.

Öffentliche Stellen sollten die Rahmenbedingungen für eine offene und transparente Verarbeitung personenbezogener Daten schaffen und für die Einhaltung der Rechte der Nutzer, insbesondere den Schutz der Privatsphäre sorgen.

Die Grundsätze spiegeln Aspekte von Medienkompetenz und Stärkung der Nutzerrechte wider, wie sie auch im deutschen Rechtsraum diskutiert werden (s. Nrn. 21.1, 21.2, 25.6).

26 Verfassungsschutz

26.1 Änderung des Verfassungsschutzgesetzes

Bereits in den zwei diesem vorangegangenen Tätigkeitsberichten (VIII. Tätigkeitsbericht, Nr. 24.4, und IX. Tätigkeitsbericht, Nr. 25.1) hatte sich der Landesbeauftragte ausführlich mit erfolgten bzw. vorgesehenen Änderungen des Verfassungsschutzgesetzes befasst. Im VIII. Tätigkeitsbericht wurde das „Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes“ vom 26. Januar 2006 (GVBl. LSA S. 12) thematisiert, welches zum Zeitpunkt der Veröffentlichung des Tätigkeitsberichtes des Landesbeauftragten bereits in Kraft war. In seinem IX. Tätigkeitsbericht stellte der Landesbeauftragte das „Zweite Gesetz zur Änderung des Gesetztes über den Verfassungsschutz im Land Sachsen-Anhalt“ vor, welches zum Zeitpunkt der Veröffentlichung des Tätigkeitsberichtes lediglich als Entwurf der Landesregierung (Drs. 5/1468neu) vorlag. Zwischenzeitlich ist aber auch dieses zweite Änderungsgesetz durch den Landtag beschlossen (GVBl. LSA 2010 S. 541) und seit dem 18. November 2010 in Kraft. Von den Bedenken, die der Landesbeauftragte gegen einzelne Regelungen des zweiten Änderungsgesetzes vortrug, fand nur ein sehr geringer Teil Eingang in die Formulierungen des Gesetzes.

Der Gesetzentwurf der Landesregierung (Drs. 5/1468neu) vom September 2009 wurde im Anschluss an seine Einbringung in das parlamentarische Verfahren viel diskutiert. Insbesondere die anlässlich der Sitzung des Ausschusses für Recht und Verfassung am 18. Februar 2009 aufgeworfenen Fragen zum Umgang der Verfassungsschutzbehörde mit personenbezogenen Daten Minderjähriger bedurften einer Klärung (s. Nr. 26.2).

In den folgenden Monaten beschäftigten sich die Parlamentarische Kontrollkommission des Landtages, das Innenministerium, die Verfassungsschutzbehörde und der Landesbeauftragte mit den Fragen bezüglich der Speicherung personenbezogener Daten Minderjähriger bei der Verfassungsschutzbehörde. Das zweite Änderungsgesetz lag solange „auf Eis“.

Nachdem der Landesbeauftragte im September 2009 seine Stellungnahme zu den Fragen um die Speicherung personenbezogener Daten Minderjähri-

ger abgegeben hatte, wäre es nach seiner Auffassung angezeigt gewesen, das zweite Änderungsgesetz nochmals vollinhaltlich zu diskutieren. Dazu kam es jedoch nicht, zumindest nicht unter Beteiligung des Landesbeauftragten.
Immerhin wurde die Befugnis der Verfassungsschutzbehörde zur Speicherung und Nutzung von Daten Minderjähriger unter 14 Jahren gestrichen, ob in elektronischer Form oder in Papierakten (§ 10).

26.2 Dokumentenmanagement beim Verfassungsschutz – Teil II

Bereits in seinem IX. Tätigkeitsbericht (Nr. 25.2) hat der Landesbeauftragte auf die sich im Rahmen der Beratungen zum „Zweiten Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt“ ergebenden Fragen zum Speichern personenbezogener Daten Minderjähriger vor Vollendung des 14. Lebensjahres in einem Dokumentenmanagementsystem beim Verfassungsschutz hingewiesen.

Der Landesbeauftragte hat sich in den vergangenen zwei Jahren intensiv mit den datenschutzrechtlichen Fragen eines Dokumentenmanagementsystems bei der Verfassungsschutzbehörde des Landes Sachsen-Anhalt an sich und der Speicherung personenbezogener Daten Minderjähriger vor Vollendung des 14. Lebensjahres in einem solchen System befasst. Da die Arbeit der Verfassungsschutzbehörde einer besonderen Vertraulichkeit unterliegt, kann an dieser Stelle nicht auf alle Feststellungen des Landesbeauftragten eingegangen werden. Dieser Beitrag soll allerdings dokumentieren, dass sich auch die Arbeit der Verfassungsschutzbehörde an datenschutzrechtlichen Vorschriften messen lassen muss und der Landesbeauftragte auf die Einhaltung dieser Vorschriften auch in diesem sensiblen Bereich hinwirkt.

Zu den Fragen nach der Rechtmäßigkeit von Speicherungen Minderjähriger vor Vollendung des 14. Lebensjahres durch die Verfassungsschutzbehörde gab der Landesbeauftragte eine Stellungnahme gegenüber dem Ausschuss für Inneres des Landtages von Sachsen-Anhalt, der Parlamentarischen Kontrollkommission, dem Innenminister und der Verfassungsschutzbehörde ab. Darin hat er nachfolgende, vom Innenminister geteilte datenschutzrechtliche Bewertung vorgenommen.

1. Bei dem Dokumentenmanagementsystem DOMEA in der Ausprägung, wie es bei der Verfassungsschutzbehörde des Landes Sachsen-Anhalt zum Einsatz kommt, handelt es sich um ein automatisiertes Verfahren und eine automatisierte Datei i. S. d. DSG-LSA.

2. Der Einsatz des Dokumentenmanagementsystems DOMEA geht sowohl in zeitlicher als auch insbesondere in inhaltlich-materieller Hinsicht weit über einen Probebetrieb hinaus. Das System ist nicht ersetzbares Arbeitsmittel zur Aufgabenerfüllung der Verfassungsschutzbehörde, weil die darin gespeicherten Erkenntnisse fast vollständig in keiner alternativen Speicherform (Papierakte) mehr vorhanden sind.

3. Für das Dokumentenmanagementsystem DOMEA wären nach DSG-LSA Festlegungen für das Verfahrensverzeichnis zu treffen gewesen. (Dies wurde nachgeholt.)

4. Der Landesbeauftragte für den Datenschutz hat den Betrieb des Dokumentenmanagementsystems zu keinem Zeitpunkt weder ausdrücklich noch durch konkludentes Handeln für datenschutzrechtlich unbedenklich erklärt, was ihm zunächst unterstellt wurde. Dies gilt insbesondere für die Einbeziehung Minderjähriger unter 14 Jahren.

5. Die Speicherung von Daten Minderjähriger unter 14 Jahren im System DOMEA entsprach bis zum 18. Februar 2009 nicht der gesetzlichen Vorgabe des § 10 Abs. 1 Satz 3 VerfSchG-LSA. Das System DOMEA fällt nicht unter den Aktenbegriff dieser Vorschrift.

6. An der materiellen Rechtmäßigkeit der Speicherung personenbezogener Daten Minderjähriger unter 14 Jahren – auch in Akten – bestehen im Hinblick auf Vorgänge vor dem 18. Februar 2009 erhebliche Zweifel.

Auch umfangreiche Erläuterungen der Verfassungsschutzbehörde vermochten die Kritik des Landesbeauftragten nicht zu zerstreuen.

Die Parlamentarische Kontrollkommission nutzte den Prüfbericht des Landesbeauftragten als Grundlage ihrer eigenen Einschätzung. Sie legte ihren Abschlussbericht im April 2010 dem Ausschuss für Inneres des Landtages von Sachsen-Anhalt vor. Dieser beriet in vertraulicher Sitzung am 26. November 2010 über den Bericht der Parlamentarischen Kontrollkommission. Dem Kurzbericht zu dieser Sitzung ist zu entnehmen, dass es „eine Verständigung zum Thema“ gab (s. Nr. 26.1).

26.3 GIAZ – Teil III

In seinem VIII. (Nr. 24.2) und IX. Tätigkeitsbericht (Nr. 25.3) hat der Landesbeauftragte das GIAZ – das Gemeinsame Informations- und Auswertungszentrum islamistischer Terrorismus – bereits vorgestellt. Er hat darüber hinaus seine rechtlichen Bedenken bezüglich der Einrichtung und der Organisationsform des GIAZ vor dem Hintergrund des Trennungsgebotes deutlich gemacht und auf einen Aspekt der Arbeit des GIAZ, die Bearbeitung von Anfragen der Ausländerbehörden, besonders hingewiesen. In Vorbereitung dieses Tätigkeitsberichtes hat der Landesbeauftragte das Ministerium des Innern des Landes Sachsen-Anhalt erneut um Stellungnahme zu nach wie vor offenen Fragestellungen gebeten.

Bezüglich der Organisation bleibt festzustellen, dass das GIAZ zwischenzeitlich aus der allgemeinen Aufbauorganisation des Landeskriminalamtes herausgenommen und als gesonderte Organisationseinheit direkt dem Abteilungsleiter 5 des Landeskriminalamtes zugeordnet wurde. Bei der Abteilung 5 des Landeskriminalamtes handelt es sich um den „Polizeilichen Staatsschutz“. Diese organisatorische Maßnahme begrüßt der Landebeauftragte, weil sie ein gewisses Maß an Trennung zwischen den eigentlichen Aufgaben des Landeskriminalamtes und denen des GIAZ mit sich bringen kann. Die innere Organisation des GIAZ wurde allerdings nicht verändert. Die durch den Landesbeauftragten insofern vorgetragenen Bedenken bestehen insbesondere auch deshalb fort, weil durch das Ministerium des Innern des Landes Sachsen-Anhalt wiederum betont wurde, dass eine Verbesserung

des Informationsaustausches zwischen Polizei und Verfassungsschutz zu verzeichnen ist. Dies dürfte nicht zuletzt dem Umstand geschuldet sein, dass der Vertreter der Verfassungsschutzbehörde im GIAZ zwischenzeitlich auch direkt im GIAZ Zugang zu allen Datenbanksystemen des Verfassungsschutzes hat und somit der Datenaustausch zwischen ihm und den Polizisten im GIAZ zusätzlich erleichtert wird. Welche Zugänge im Einzelnen bestehen, muss hier aus Gründen der Vertraulichkeit offen bleiben.

In Bezug auf die Bearbeitung von Anfragen der Ausländerbehörden kann jedoch aus datenschutzrechtlicher Sicht ein zumindest kleiner Achtungserfolg vermeldet werden. Der Landesbeauftragte hatte in der Vergangenheit bemängelt, dass alle Anfragen der Ausländerbehörden im GIAZ bearbeitet werden. Weil nach Auffassung des Landesbeauftragten nicht alle Anfragen für die Informationsgewinnung und Auswertung zu Fragen des islamistischen Terrorismus relevant sein dürften, sollte sichergestellt werden, dass nur solche Anfragen von Ausländerbehörden im GIAZ bearbeitet werden, bei denen ein Bezug zum islamistischen Terrorismus zu befürchten steht. Durch eine Veränderung in der Ablauforganisation im Landeskriminalamt wurde zwischenzeitlich erreicht, dass die Anfragen der Ausländerbehörden grundsätzlich von einer Organisationseinheit der allgemeinen Aufbauorganisation des Landeskriminalamtes und nicht dem GIAZ bearbeitet werden. Nur solche Anfragen, bei denen sich Verdachtsmomente zum islamistischen Extremismus oder Terrorismus ergeben, werden vom GIAZ mit bearbeitet.

Der Landesbeauftragte wird die Entwicklung im und um das GIAZ auch in den kommenden Jahren weiter beobachten und begleiten. Auch wenn aus datenschutzrechtlicher Sicht Verbesserungen erreicht werden konnten, sind die Bedenken des Landesbeauftragten noch nicht ausgeräumt.

Auf Bundesebene existiert das dem GIAZ vergleichbare GTAZ, das Gemeinsame Terrorismusabwehrzentrum. Zusätzlich zu diesen bestehenden Strukturen ist nach Vorstellung des Bundesinnenministers ein Cyber-Abwehrzentrum gebildet worden, für welches das GTAZ strukturell Pate stand. Gegebenenfalls werden hier neue Einrichtungen geschaffen, die an denselben strukturellen Defiziten in Bezug auf das Trennungsgebot leiden, wie bereits bestehende.

26.4 Widerspruch gegen die Einsicht in Sicherheitsüberprüfungsakten

Nach § 22 Abs. 3 DSG-LSA findet eine datenschutzrechtliche Kontrolle durch den Landesbeauftragten nicht statt, wenn sie sich auf personenbezogene Daten erstreckt, die sich in Akten über die Sicherheitsüberprüfung befinden und der Betroffene generell oder im Einzelfall der Kontrolle der auf ihn bezogenen Daten widersprochen hat. Der Widerspruch ist gegenüber dem Landesbeauftragten für den Datenschutz zu erklären. Die Umsetzung dieser Vorschrift hat den Landesbeauftragten in den vergangenen zwei Jahren beschäftigt.

Eine Sicherheitsüberprüfung wird für Personen durchgeführt, die sicherheitsempfindliche Tätigkeiten ausüben und damit z. B. Zugang zu Verschlusssachen bekommen sollen. Sie ist in jedem Fall ein bedeutender Einschnitt in die Privatsphäre des Betroffenen. Er hat diverse Angaben zu seiner Person

zu machen. Aber auch Ehegatten, Lebenspartner und Lebensgefährten können mit in die Überprüfung einbezogen werden. Letztendlich können in den so entstandenen Akten der Sicherheitsüberprüfung eine Menge auch sehr persönlicher Angaben enthalten sein. Zwar erfolgt eine Sicherheitsüberprüfung grundsätzlich nur mit Einverständnis des Betroffenen und die Unterlagen unterliegen besonderen Zugangsvoraussetzungen, trotzdem haben Betroffene ggf. ein Interesse daran, dass so wenig Personen wie möglich Zugang zu diesen Unterlagen erlangen. Diese Betroffenen können den Zugang des Landesbeauftragten zu den Akten der Sicherheitsüberprüfung durch das Erklären ihres Widerspruchs verhindern. In diesen Fällen kann dann zwar keine datenschutzrechtliche Kontrolle stattfinden; in der Kenntnis dieser Konsequenz bleibt es jedoch dem Betroffenen überlassen, ob er von seinem Widerspruchsrecht Gebrauch macht.

Den Eingang einer solchen Widerspruchserklärung eines Betroffenen nahm der Landesbeauftragte zum Anlass, das Verfahren der Sicherheitsüberprüfung und die verwendeten Formblätter einer Kontrolle zu unterziehen. Dabei musste festgestellt werden, dass die Praxis der vergangenen Jahre nicht mit der Rechtslage vereinbar ist. Der Landesbeauftragte hat sich daraufhin mit dem Ministerium des Innern des Landes Sachsen-Anhalt in Verbindung gesetzt und um die Anpassung des Verfahrens und der Formblätter gebeten. Im Nachgang zu dieser Bitte waren noch einige Gespräche und diverser Schriftwechsel zu führen, bis zwischen dem Ministerium und dem Landesbeauftragten Einvernehmen bezüglich des Verfahrens hergestellt werden konnte. Dann erfolgte die Umsetzung des Vereinbarten jedoch zeitnah.

Zwischenzeitlich hat das Ministerium des Innern des Landes Sachsen-Anhalt das Verfahren an die Rechtslage angepasst und die Formblätter überarbeitet. Alle Stellen, die mit dem Sicherheitsüberprüfungsgesetz des Landes Sachsen-Anhalt zu Fragen der Sicherheitsüberprüfung befasst sind, wurden vom Ministerium auf die veränderte Sachlage hingewiesen. Für die Zukunft konnte so rechtskonformes Handeln sichergestellt werden. Auch für die Bereinigung für die zurückliegenden Jahre fand sich eine zufriedenstellende Lösung.

26.5 NADIS-neu

Anlässlich ihrer 80. Tagung im November 2010 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung gefasst, die sich gegen die Schaffung der Möglichkeit einer Volltextsuche in Dateien der Sicherheitsbehörden richtet (**Anlage 17**). Die Sicherheitsbehörden bauen derzeit ihre elektronischen Systeme mit dem Ziel aus, die bisher nur in Akten vorhandenen Daten einer umfassenden Volltextverarbeitung mit Suchmöglichkeiten zugänglich zu machen. Die Datenschutzbeauftragten haben ihre Bedenken hinsichtlich der Gefahren, die diese Auswertungsmöglichkeiten bieten, mit ihrer Entschließung deutlich gemacht. Besonderes Augenmerk haben sie dabei auch auf die besondere Bedeutung von Volltextrechercheмöglichkeiten im Bereich der Nachrichtendienste gelegt.

Ein solches den Nachrichtendiensten zur Verfügung stehendes System ist NADIS, das Nachrichtendienstliche Informationssystem. Bei NADIS handelt es sich um ein bereits seit Jahrzehnten bestehendes automatisiertes Daten-

verbundsystem, an dem die Verfassungsschutzbehörden des Bundes und der Länder beteiligt sind. Im Grunde ist die Zusammenarbeit der Verfassungsschutzbehörden auf technischer Ebene der Zusammenarbeit der Polizeien sehr ähnlich (s. Nr. 19.8).

Bisher werden in NADIS nur Angaben zu NADIS-relevanten Personen gespeichert. Zugriffsberechtigte können in NADIS auch nur nach diesen Personen suchen. Im Falle eines Treffers muss sich die suchende Verfassungsschutzbehörde dann an die Behörde wenden, welche die Angaben zur Person in NADIS eingestellt hat. Bei dieser Behörde können dann auf konventionellem Wege Erkenntnisse eingeholt werden, soweit dafür eine rechtliche Grundlage besteht. Bei der Anfrage auf konventionellem Weg prüft sowohl die anfragende als auch die angefragte Verfassungsschutzbehörde zwangsläufig die Zulässigkeit der Anfrage bzw. die Übermittlung von Daten.

NADIS soll nun aber überarbeitet, den heutigen Bedürfnissen der Arbeit von Verfassungsschutzbehörden angepasst werden. Dazu soll in NADIS-neu u. a. die Möglichkeit zum Speichern von Dokumenten und deren Suchfähigkeit integriert werden. Zukünftig soll nicht mehr nur eine bestimmte Person gesucht werden können, sondern im Falle eines Treffers sollen auch die zu dieser Person elektronisch abgelegten Dokumente geöffnet und durchsucht werden können. Das Einstellen solcher Dokumente stellt datenschutzrechtlich ein deutlich höheres Gefährdungspotenzial für die personenbezogenen Daten dar, als die bisherige Verfahrensweise, zumal die Behörde, die die Dokumente eingestellt hat, den Zugriff auf diese nur noch sehr eingeschränkt kontrollieren kann.

Der Landesbeauftragte wird die Entwicklung von NADIS-neu weiterhin begleiten und, soweit Entscheidungskompetenzen der Verfassungsschutzbehörde des Landes Sachsen-Anhalt betroffen sind, auf die datenschutzgerechte Ausgestaltung der bestehenden Möglichkeiten hinwirken.

27 Verkehr

27.1 Online-Anbindung der Fahrerlaubnisbehörden an das KBA

Der Landesbeauftragte hat in seinem IX. Tätigkeitsbericht (Nr. 26.1) von seinen Bemühungen berichtet, die mit der Online-Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt (KBA) aus datenschutzrechtlicher Sicht notwendigen Gesetzesänderungen im Straßenverkehrsgesetz (StVG) und der Fahrerlaubnisverordnung (FeV) mit auf den Weg zu bringen. Die Zuständigkeit liegt hier allerdings beim Bundesministerium für Verkehr, Bau und Stadtentwicklung. Diesem liegt seit Ende 2007 das Gutachten vom 19. Oktober 2007 vor, das vom Arbeitskreis Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK Verkehr) erarbeitet wurde.

Zwischenzeitlich wurde auf Initiative der Länder mit einem Gesetz zur Änderung des StVG vom 3. Februar 2009 (BGBl. I S. 150) bereits die Frist zur Auflösung der örtlichen Fahrerlaubnisregister in § 65 Abs. 10 Satz 2 StVG bis zum 31. Dezember 2012 verlängert, da absehbar wurde, dass die bis dato festgelegte Frist (31.12.2006) nicht einzuhalten war, um die Daten aller

Fahrerlaubnisbehörden in Deutschland in das Zentrale Fahrerlaubnisregister (ZFER) des KBA zu übernehmen.

Im Bund-Länder Fachausschuss Fahrerlaubnis-/Fahrlehrerrecht (BLFA-FE/FL) wurde erst im September 2009 unter Berücksichtigung des o. g. Gutachtens im Zuge des Gesetzgebungsverfahrens zur Änderung des StVG ein entsprechender Mehrheitsbeschluss gefasst, dem sich das Bundesverkehrsministerium „zu beugen“ hatte (so seine Begründung gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit). Für die Nichtberücksichtigung der datenschutzrechtlichen Forderungen im Gesetzentwurf wurden so wiederum die Länder verantwortlich gemacht.

In ihrer Stellungnahme zum IX. Tätigkeitsbericht des Landesbeauftragten (LT-Drs. 5/2385) verwies die Landesregierung darauf, dass die im Gutachten geforderte Datenanbindung und der Datenaustausch mittels qualifizierter elektronischer Signatur mit einem erheblichen Kostenaufwand, insbesondere für die kommunalen Fahrerlaubnisbehörden, verbunden wären. Auch hätte das Ministerium für Landesentwicklung und Verkehr keine direkte Einflussmöglichkeit auf die technische Ausstattung der Fahrerlaubnisbehörden im Land. Es wollte den Landesbeauftragten zeitnah über den Beratungsstand unterrichten und bei der Meinungsbildung des Landes einbeziehen.

Das Ergebnis der Meinungsbildung im BLFA-FE/FL wurde dem Landesbeauftragten nicht mitgeteilt. Das Landesverkehrsministerium hatte aber dem Landesbeauftragten bereits im März 2010 die Möglichkeit gegeben, im Vorgriff auf die geplante StVG-Novelle zu einem Referentenentwurf des Bundes Stellung zu nehmen. Der Landesbeauftragte war der Meinung, dass dieser Referentenentwurf die grundsätzlichen Probleme bei der Online-Anbindung der Fahrerlaubnisbehörden an das KBA und die Probleme bezüglich der dortigen, ausschließlichen elektronischen Speicherung im ZFER nach Wegfall der örtlichen Fahrerlaubnisregister aus datenschutzrechlicher Sicht nicht lösen würde.

Zur gleichen Einschätzung kam der Landesbeauftragte bei dem im Juli 2010 zugeleiteten Referentenentwurf, der sich inhaltlich aber nicht vom vorherigen unterschied. Das Landesverkehrsministerium wurde aus diesem Grund über die mit den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im AK Verkehr abgestimmte Stellungnahme gegenüber dem Bund informiert.

Über den weiteren Verlauf des Gesetzgebungsverfahrens zum StVG wurde der Landesbeauftragte nicht mehr informiert. Der Bundesgesetzgeber hatte allerdings überraschend zum Jahresende 2010 eine Änderung des StVG vorgenommen. Nach den erfolgreichen Pilotprojekten des Modellversuches „Begleitetes Fahren ab 17“ in den Ländern wurde neben der dauerhaften Übernahme dieses Modells in das StVG (§ 6e) gleichzeitig die Gelegenheit genutzt, auch die Änderung des StVG (§§ 51, 53, 54) vorzunehmen, angeblich unter Berücksichtigung der Beanstandung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aus seiner Kontrolle des ZFER beim KBA aus dem Jahr 2008 und des Gutachtens des AK Verkehr.

Mit dem Gesetz zur Änderung des Straßenverkehrsgesetzes vom 2. Dezember 2010 (BGBl. I S. 1748) wurde allerdings nur die bisherige ungesetzliche Protokollierungspraxis des KBA legalisiert (§ 53 Abs. 3 und 4 StVG) und die Gesetzeslage der Praxis angepasst, da mittlerweile bereits von vielen Fahrerlaubnisbehörden direkt im ZFER des KBA die Änderungen der Daten vorgenommen werden. Das bedeutet, dass in der Praxis gar keine Übermittlung mehr an das KBA erfolgt, denn die inhaltliche Verantwortung für die geänderten Daten trägt allein die jeweilige Fahrerlaubnisbehörde. Bei einer Übermittlung (Mitteilung nach § 51 StVG) müsste eigentlich das KBA als selbstständige Behörde tätig werden, das ist aber bei Nutzung der in § 53 Abs. 1a StVG („Datenfernübertragung durch Direkteinstellung“) eröffneten Möglichkeit der unmittelbaren und direkten Änderung des eigenen Datenbestandes durch die jeweilige Fahrerlaubnisbehörde nicht mehr der Fall. Leider hat der Bundesgesetzgeber noch immer nicht berücksichtigt, dass sich das ZFER nach Wegfall bzw. Auflösung der örtlichen Fahrerlaubnisregister zu einer Verbunddatei wandeln wird, für die normenklare Regelungen der Verantwortlichkeiten zwischen den Fahrerlaubnisbehörden und dem KBA, auch aus datenschutzrechtlicher Sicht, zu treffen sind.

Diese insgesamt seither festzustellende eher zögerliche Reaktion des Bundes, aber auch der Länder, zur Umsetzung der datenschutzrechtlichen Forderungen bei der Neugestaltung der technischen wie rechtlichen Rahmenbedingungen bei der Online-Anbindung der Fahrerlaubnisbehörden an das ZFER veranlasste den AK Verkehr, dieses Thema wieder auf die Tagesordnung seiner Beratung im Mai 2011 zu setzen. Im Ergebnis dieser Arbeitskreissitzung ist festzustellen, dass die Forderungen der Datenschutzbeauftragten des Bundes und der Länder nach Gewährleistung einer sicheren, integeren, authentischen, revisionsfähigen und transparenten Verarbeitung der Fahrerlaubnisdaten bei der Übermittlung zum und der Langzeitspeicherung im ZFER bisher nur unzureichend vom Bundesgesetzgeber berücksichtigt worden sind.

27.2 Verkehrsüberwachung mittels Videoaufzeichnung

Das Bundesverfassungsgericht (BVerfG) hatte mit seinem Beschluss vom 11. August 2009 (2 BvR 941/08, NJW 2009, 3293) festgestellt, dass eine Geschwindigkeitsmessung mittels einer Videoaufzeichnung, gestützt ausschließlich auf einen **Erlass** eines Ministeriums ohne weitere Rechtsgrundlage, einer verfassungsrechtlichen Prüfung nicht standhält. Dem entgegen stehende Entscheidungen vorinstanzlicher Gerichte seien unter keinem rechtlichen Aspekt vertretbar und damit willkürlich. Diese Entscheidung des BVerfG hatte damit über den verhandelten Einzelfall aus Mecklenburg-Vorpommern hinaus eine grundlegende Bedeutung für alle Maßnahmen der Verkehrsüberwachung durch die kommunalen Ordnungsbehörden der Landkreise und kreisfreien Städte sowie der Polizeien der Länder. Demnach bedarf die präventive Verkehrsüberwachung mittels Videoaufzeichnung einer verfassungsmäßigen rechtlichen Grundlage.

Bereits in seinem IX. Tätigkeitsbericht (Nr. 26.2) hatte sich der Landesbeauftragte mit diesem Thema beschäftigt und eine ähnliche Auffassung vertreten wie das BVerfG. Im damals vorliegenden Fall der Verkehrsüberwachung erfolgte die Videoaufzeichnung mittels des sogenannten Verkehrs-Kontroll-

Systems (VKS). Die Untersuchung der damaligen Praxis dieser Videoaufzeichnungen mit dem VKS durch das Ministerium des Innern ergab, dass die Videoaufzeichnungen zum Teil auch im **Dauerbetrieb** erfolgten. Diese Aufzeichnungsweise war datenschutzrechtlich unzulässig. Dieser Meinung war auch das Ministerium des Innern in seiner Stellungnahme an den Landesbeauftragten. Mit einem Erlass vom 13. Juli 2007 hatte es damals die Polizeibehörden angewiesen, den Einsatz der Geräte nur im rechtlich zulässigen Umfang vorzunehmen. Danach ist die verdachtsunabhängige Videoaufzeichnung im Dauerbetrieb nicht statthaft. Erst bei Vorliegen eines **Anfangsverdachts** im Messfeld darf der den Verkehrsablauf beobachtende Polizeibeamte die Videoaufzeichnung starten und muss diese dann auch nach der Beweisaufnahme wieder beenden.

Nach Würdigung der BVerfG-Entscheidung vertrat der Landesbeauftragte den Standpunkt, dass es selbst bei Vorliegen eines Anfangsverdachts für eine Verkehrsordnungswidrigkeit oder gar Verkehrsstraftat für eine Videoaufzeichnung des Geschehens einer Rechtsgrundlage bedarf. Der Landesbeauftragte hatte deshalb das Ministerium des Innern im September 2009 um Mitteilung gebeten, auf welcher Rechtsgrundlage in Sachsen-Anhalt Maßnahmen der Videoüberwachung im Straßenverkehr durch die Landkreise, kreisfreien Städte und die Polizei durchgeführt werden.

Vor dem Hintergrund des o. g. Beschlusses des BVerfG hatte das Ministerium des Innern in einem Erlass vom 26. August 2009 nochmals auf seinen Runderlass vom 6. März 2009 (Verkehrsüberwachungserlass, MBl. LSA S. 208) verwiesen und darin erneut klar gestellt, dass verdachtsunabhängige Videoaufzeichnungen im Dauerbetrieb, bei denen nicht verdächtige Personen erfasst werden, nicht zulässig sind. Auch in Sachsen-Anhalt gab es zum damaligen Zeitpunkt hierzu also nur den sogenannten Verkehrsüberwachungserlass für eine Geschwindigkeitsmessung mittels einer Videoaufzeichnung. Damit fehlte es hier (noch) an einer geeigneten Rechtsgrundlage. Weder § 30 DSG-LSA noch § 16 SOG LSA sind im Übrigen einschlägig.

Darüber hinaus wurde mit Erlass des Ministeriums des Innern vom 13. Juli 2007, der Bezug auf ein Schreiben des Ministeriums des Innern an den Landesbeauftragten vom 8. Dezember 1995 nimmt, festgelegt, dass „... *ein Dauerbetrieb der Videokameras unzulässig wäre.“* Der Aufzeichnungsbetrieb habe sich auf Gegebenheiten „... *bei Vorliegen eines Anfangsverdachtes* ...“ zu beschränken. Damit werden Aufzeichnungen von Daten unbeteiligter oder die Vorschriften der Straßenverkehrsordnung beachtender Dritter auf ein technisch unvermeidbares Minimum reduziert. Darüber hinaus wären sie unzulässig.

Auch in Sachsen-Anhalt hatte der Beschluss des BVerfG vom 11. August 2009 für Aufsehen und zudem für Unsicherheiten in der Praxis der Verkehrsüberwachung mittels Videoaufzeichnung geführt. Entsprechende Anfragen erreichten auch den Landesbeauftragten.

Im Interesse einer höheren Rechtssicherheit aller Beteiligten hatte der Landesbeauftragte die Schaffung einer geeigneten Rechtsgrundlage angeregt.

Erst mit zwei weiteren Beschlüssen im Jahr 2010 hat das BVerfG für eine nicht ganz unumstrittene Rechtsklarheit gesorgt, insbesondere was die Rechtsgrundlage für die Erhebung und Verarbeitung von Daten bei Verkehrsüberwachungen mit sogenannten bildgebenden Messverfahren zur Feststellung von Geschwindigkeits- oder Abstandsverstößen mittels Videoaufzeichnungen und die Anfertigung von Frontfotos bei begangenen Verkehrsordnungswidrigkeiten betraf.
Mit den Beschlüssen vom 5. Juli 2010 (2 BvR 759/19) – Verfassungsbeschwerde gegen „Blitzer“ erfolglos – und vom 12. August 2010 (2 BvR 1447/10) – Verfassungsbeschwerde gegen Anfertigung von Videoaufnahmen zum Beweis von Verkehrsverstößen erfolglos – hatte das BVerfG festgestellt, dass es verfassungsrechtlich nicht zu beanstanden ist, die Vorschrift des § 100h Abs. 1 Satz 1 Nr. 1 StPO i. V. m. § 46 Abs. 1 OWiG als Rechtsgrundlage für die Anfertigung von Bildaufnahmen und von Videoaufzeichnungen heranzuziehen. Diese hatte zuvor schon das Ministerium des Innern gegenüber dem Landesbeauftragten als einschlägig angesehen.

Die Botschaft aus den Entscheidungen des BVerfG ist aber deutlich. Eine **anlasslose** Verkehrsüberwachung mittels Videoaufzeichnung bzw. Bildaufnahme zu repressiven Zwecken ist verfassungswidrig.

27.3 Verkehrszählung zur Ermittlung des Durchgangsverkehrs

Der Landesbeauftragte war im zurückliegenden Berichtszeitraum mehrfach von Petenten, aber auch von öffentlichen Stellen zum Thema Nutzung von Videotechnik bei verkehrsplanerischen Aufgaben, wie z. B. bei Verkehrszählungen, angefragt worden.

Im Fall einer großen kreisfreien Stadt erfuhr der Landesbeauftragte im Mai 2009 erst durch eine Anfrage der Presse von einer am nächsten Tag stattfindenden umfangreichen Verkehrszählung zum Durchgangsverkehr unter Beteiligung eines privaten Auftragnehmers. Eine Prüfung des Ablaufes der Verkehrszählung selbst konnte damals durch den Landesbeauftragten nicht mehr unmittelbar durchgeführt werden. Aus diesem Grund wurde die Stadt zu einer Stellungnahme aufgefordert. Die Fragen des Landesbeauftragten betrafen daher schwerpunktmäßig die Umsetzung der technischen und organisatorischen Maßnahmen bei dieser umfangreichen Verkehrszählung. § 8 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) räumt einer öffentlichen Stelle die Möglichkeit ein, personenbezogene Daten im Auftrag, auch durch Private, erheben, verarbeiten und nutzen zu lassen.

Aus dem Antwortschreiben der Stadt wurde ersichtlich, dass die Planungsvorbereitungen für die Verkehrszählung des Durchgangsverkehrs an 17 Messstellen bereits im März 2007 begonnen wurden. Spätestens nach der Zuschlagserteilung am 2. April 2009 wäre die Unterrichtung des Landesbeauftragten gemäß § 8 Abs. 6 Satz 2 DSG-LSA erforderlich gewesen, da es sich um einen privaten Auftragnehmer gehandelt hatte und durch die Stadt vertraglich die Kontrollrechte des Landesbeauftragten dem Auftragnehmer gegenüber sicherzustellen waren. Üblicherweise erhält der Landesbeauftragte bei einer solchen Unterrichtung den Vertrag zu dieser Auftragsdatenverarbeitung zur Überprüfung. Von einer rechtzeitigen Einbeziehung des Landesbeauftragten konnte daher keine Rede sein.

Der Gesetzgeber hat in § 8 Abs. 2 DSG-LSA die Pflichten der öffentlichen Stelle als Auftraggeber, insbesondere hinsichtlich der Auswahl des Auftragnehmers, festgelegt.

Die Antwort der Stadt erreichte den Landesbeauftragten trotz mehrmaliger Mahnung erst im Oktober 2009 und konnte nicht alle aufgeworfenen Fragestellungen letztendlich befriedigend beantworten. Insbesondere blieb die Mitwirkung der EDV-Verantwortlichen der Stadt oder des EDV-Dienstleisters in Bezug auf die Prüfung des eingesetzten Programms, dessen Sicherheitsfunktionen und der weiteren getroffenen technischen und organisatorischen Maßnahmen zur Absicherung dieser Verkehrszählung unklar.

Der Landesbeauftragte berücksichtigte bei seiner Bewertung aber die Tatsache, dass die Verkehrszählung bereits seit Monaten abgeschlossen und die dabei erhobenen personenbezogenen Daten ordnungsgemäß durch den Auftragnehmer gelöscht wurden, und abschließend insbesondere, dass

- die erhobenen amtlichen Kennzeichen an allen 17 Messstellen in pseudonymisierter Form gespeichert wurden,

- die erhobenen amtlichen Kennzeichen nur für die Verkehrszählungszwecke verarbeitet und genutzt wurden und keine Datenübermittlung an Dritte erfolgte,

- der Stadt danach nur anonymisierte, statistische Daten zu weiteren Verwendung für Verkehrsplanungszwecke vorlagen.

Die pseudonymisierte Erfassung (§ 2 Abs. 7a DSG-LSA) amtlicher Kennzeichen kann bei weiteren flankierenden technischen und organisatorischen Datensicherheitsmaßnahmen den Belangen des Datenschutzes Rechnung tragen.

Die in ihrer Antwort detaillierte Darstellung zur Vorbereitung und zum Ablauf der Verkehrszählung lies das Bemühen der Stadt erkennen, auch datenschutzrechtliche Belange berücksichtigt zu haben. Allerdings können z. B. vorgelegte eigene Referenzen eines potentiellen Auftragnehmers für die öffentliche Stelle nur ein Anhaltspunkt für die besondere Zuverlässigkeit und Eignung sein. Es entbindet sie in keinem Fall von der eigenen Prüfung der Wirksamkeit der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

Eine Beauftragung privater Dritter zur Aufgabenerfüllung öffentlicher Stellen in Sachsen-Anhalt ist unter Einhaltung der Regelungen des § 8 DSG-LSA möglich. Nach § 8 Abs. 2 Satz 1 DSG-LSA kommt der sorgfältigen Auswahl des Auftragnehmers durch die öffentliche Stelle, unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen, eine besondere Bedeutung zu. Die Einbeziehung eigenen oder externen EDV-Sachverstandes durch die öffentliche Stelle ist dabei unabdingbar.

Die Stadt war trotz Beauftragung eines privaten Auftragnehmers die für die Erhebung, Verarbeitung und Nutzung verantwortliche Stelle (§ 8 Abs. 1 DSG-

LSA). Als Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten (hier die Aufzeichnung amtlicher Kennzeichen von Fahrzeugen mittels Videotechnik für nicht repressive Zwecke) kann § 9 Abs. 1 DSG-LSA i. V. m. § 10 Abs. 1 DSG-LSA herangezogen werden. Die Videoaufzeichnung von amtlichen Kennzeichen ist hier nicht das Ziel der Maßnahme der öffentlichen Stelle, sondern bei dieser umfassenden Verkehrszählung Mittel zum Zweck. Aus diesem Grund kam den getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers nach Prüfung durch die öffentliche Stelle eine besondere Bedeutung zu.

Unter Beachtung der bereits länger zurückliegenden und abgeschlossenen Verkehrszählung, der Versicherung der Löschung der personenbezogenen Daten beim Auftragnehmer unter Kontrolle der behördlichen Datenschutzbeauftragten und dem zumindest erkennbaren Bemühen der Stadt zur Berücksichtigung der datenschutzrechtlichen Belange, sah der Landesbeauftragte von einer Beanstandung gemäß § 24 Abs. 3 DSG-LSA ab. Der Landesbeauftragte geht davon aus, dass die Stadt zukünftig, insbesondere bei der Auftragsvergabe an private Unternehmen, der Umsetzung des § 8 Abs. 2 und Abs. 6 DSG-LSA besondere Aufmerksamkeit schenkt.

Der Meinungsbildungsprozess, inwieweit die allgemeinen Regelungen eines subsidiär wirkenden Landesdatenschutzgesetzes (hier: DSG-LSA) für eine solche nicht repressive Datenerhebung und -verarbeitung mittels Videotechnik vom amtlichen Kennzeichen (also personenbezogenen Daten) im Lichte der Rechtsprechung des Bundesverfassungsgerichts zur Verkehrsüberwachung mittels Videoaufzeichnung (s. Nr. 27.2) als Rechtsgrundlage herangezogen werden können, ist allerdings auch im Kreis der Landesdatenschutzbeauftragten noch nicht abgeschlossen.

Der Einsatz von Videotechnik erfolgt nach Kenntnis des Landesbeauftragten schon seit langem durch private Firmen, die im Bereich der Verkehrszählung und Verkehrsplanung tätig sind. Hier ist nach Meinung des Landesbeauftragten der Gesetzgeber gefordert, die Notwendigkeit einer speziellen Rechtsgrundlage für Videoaufzeichnungen personenbezogener Daten zu nicht repressiven Zwecken (u. a. von amtlichen Kennzeichen) zu prüfen. Die Zeiten, wo z. B. Scharen von Rentnern mit Bleistift und Papier an Kreuzungen komplexe Verkehrszählungen durchführen, dürften wohl mittlerweile vorbei sein und die Ausnahme darstellen.

28 Wahlen

28.1 Videoüberwachung von Wahllokalen

Im Zusammenhang mit einer Antwort der Bundesregierung auf eine Kleine Anfrage der Linken zur Videoüberwachung von Wahllokalen (BT-Drs. 17/1140) ermittelte der Landesbeauftragte, inwieweit diese Thematik auch in Sachsen-Anhalt eine Rolle spielte.

Hintergrund war, dass bei der Bundestagswahl 2009 Wahllokale in mit Videokameras ausgestatteten Räumen eingerichtet worden waren und die Gefahr bestand, dass das Wahlgeheimnis nicht sichergestellt gewesen sei.

Das Innenministerium teilte hierzu mit, dass drei Wahllokale in Filialen einer Bank mit installierten Videokameras eingerichtet worden waren. Die Videokameras seien weder auf die Wahlkabinen noch auf die Wahlurne gerichtet gewesen. Entsprechende Hinweisschilder, dass die Bankfilialen videoüberwacht werden, waren sichtbar angebracht.

Zwei weitere Wahllokale waren in Räumlichkeiten von videoüberwachten Feuerwehren eingerichtet. Die Kameras waren für den Zeitraum der Wahl ausgeschaltet. Die Kameras wurden zusätzlich mit lichtundurchlässigem Material abgedeckt.

In allen fünf Fällen kam es zu keiner Beschwerde.

Aus Sicht des Landesbeauftragten waren die beschriebenen Abläufe nicht zu beanstanden. Der Landesbeauftragte bat auch künftig darauf zu achten, dass bei der Einrichtung von Wahllokalen in Räumlichkeiten mit installierten Videokameras das Wahlgeheimnis gewahrt bleibt.

Anlagenverzeichnis

Anlage 1

Eckpunktepapier 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;

- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;

- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;

- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;

- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;

- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;

- die Videoüberwachung in Staat und Gesellschaft einzuschränken;

- den Schutz der Meldedaten zu verbessern;

- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

Anlage 2

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Anlage 3

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

Anlage 4

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

Anlage 5

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST – im weiteren Verfahren einzusetzen.

Anlage 6

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin

"Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mit verfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleiben oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality"-Reportagen Abstand zu nehmen.

Anlage 7

Eckpunktepapier 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Ein modernes Datenschutzrecht für das 21. Jahrhundert (Zusammenfassung)

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Daten-

schutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

Anlage 8

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Anlage 9

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Anlage 10

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden:

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberech-

tigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),

- die Leistung, Wirkung sowie der Erfolg und die Effizienz,

- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

Anlage 11

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

Anlage 12

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

- Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

- Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

- Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

- Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Anlage 13

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Ein-

druck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.

- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Erweiterung der zentralen Steuerdatenbank um elektronische Lohnsteuerabzugsmerkmale (ELStAM) vom 24. Juni 2010

Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer: Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat: In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs: Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept: Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-

Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

Anlage 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010

Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

Anlage 16

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. November 2010 in Freiburg im Breisgau

Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass:

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Anlage 17

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. November 2010 in Freiburg im Breisgau

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung

noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

Anlage 18

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. November 2010 in Freiburg im Breisgau

Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inan-

spruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

Anlage 19

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2011 in Würzburg

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
    - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
    - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
    - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.
- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.
- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.
- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere

    - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.

    - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

    - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,

    - zur privaten Nutzung von Telekommunikationsdiensten,

    - zum Thema Whistleblowing,

    - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,

    - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,

    - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Anlage 20

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2011 in Würzburg

Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, 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.

Anlage 21

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2011 in Würzburg

Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

Anlage 22

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2011 in Würzburg

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

Anlage 23

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2011 in Würzburg

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

- Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

- Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

- Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

- Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

- Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

- Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

- Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

- nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Anlage 24

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 26./27. November 2009 in Stralsund

Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.

- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

Anlage 25

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 24./25. November 2010 in Düsseldorf

Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.

- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

Anlage 26

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 24./25. November 2010 in Düsseldorf

Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

Anlage 27

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 24./25. November 2010 in Düsseldorf

Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB. Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle

    - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

    - umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,

    - Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

    - Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,

- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),

- betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),

- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und

- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse bereits zum Zeitpunkt der Bestellung zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit

der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1-2 Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.

3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.

4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.

5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

Anlage 28

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 8. April 2011

Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.
- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

Anlage 29

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 4./5. Mai 2011 in Düsseldorf

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

Anlage 30

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 4./5. Mai 2011 in Düsseldorf

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

- Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

- Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

- Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

- Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

- Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

- Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

- Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

- nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Anlage 31

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 4./5. Mai 2011 in Düsseldorf

Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“.

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

- Transparenz bezüglich der Preisgabe personenbezogener Daten: In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten: Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

- Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung: Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindes-

tens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

- Anonyme und pseudonyme Nutzungsmöglichkeiten: Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design vom 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport).

Anlage 32

Europäische Datenschutzkonferenz am 23./24. April 2009 in Edinburgh

Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa

Europa hat eine lange und stolze Geschichte von Standards und Gesetzgebung im Bereich des Datenschutzes. Einige davon wurden im Laufe der Zeit geändert und andere werden unter Beobachtung bleiben. Die Gesetzgebung folgt immer dem technischen und sozialen Fortschritt und es ist für die Datenschutzbehörden eine Herausforderung, mit diesen Entwicklungen Schritt zu halten und angesichts dieser sich schnell ändernden Umstände die Gesetze anzuwenden und eine Strategie zu entwickeln.

Datenschutzrechtliche Standards und Gesetzgebung entwickeln sich auch zügig in den restlichen Teilen der Welt und Europa spielte aufgrund seiner beratenden und unterstützenden Tätigkeit eine wichtige Rolle in einigen Ländern. Obwohl die bestehenden Standards und Gesetzgebungen Unterschiede in bestimmten Bereichen aufweisen können, zielen sie letzten Endes doch alle auf den Schutz personenbezogener Daten und die Rechte und Freiheiten der Einzelnen ab.

Die Konferenz verpflichtet sich, einen Beitrag für die Entwicklung des Datenschutzes in Europa zu leisten und dafür zu sorgen, dass aus den Erfahrungen der europäischen Länder Nutzen für die weltweite Diskussion über den Datenschutz gezogen wird. Dazu gehört auch die bessere Umsetzung und Durchsetzung des bestehenden Rechtsrahmens.

Die europäischen Datenschutzbeauftragten stehen zu ihrer Führungsrolle in der Zukunft. Dementsprechend erwartet die Konferenz, dass die Datenschutzbeauftragten einen konstruktiven Beitrag zu den laufenden Arbeiten und Initiativen leisten, die darauf abzielen, die Diskussion über die Zukunft des Datenschutzes in Europa und insbesondere über den zukünftigen Rechtsrahmen voranzubringen.

Die Konferenz wird sich weiterhin für die Notwendigkeit von hohen Datenschutzstandards in allen Lebensbereichen einsetzen, insbesondere in Bezug auf technologische Entwicklungen, die Online-Welt und Strafverfolgungsmaßnahmen.

Die Konferenz unterstützt die Entwicklung und Verbesserung einer umfassenden Gesetzgebung zum Datenschutz, die

- die Grundrechte und Freiheiten gewährleistet und fördert;
- auf bestehenden Datenschutzgrundsätzen aufbaut;
- Wert darauf legt, dass die angestrebten Ergebnisse in der Praxis auf effektive Art und Weise erreicht werden;
- Organisationen ermutigt, beste Praktiken zu übernehmen, wie etwa „privacy by design“ (eingebauter Datenschutz);
- die Risiken schädlicher Auswirkungen angeht, denen der Einzelne und die Gesellschaft insgesamt ausgesetzt sind;

- nicht zu rechtfertigende Belastungen vermeidet und
- für eine effektive Durchsetzung sorgt.

Die Konferenz ruft alle auf, die an Diskussionen über Strategien und Gesetze zum Datenschutz beteiligt sind, sich mit den Gemeinsamkeiten statt mit den Unterschieden verschiedener Regelwerke und Rahmenwerke zu befassen und nach Wegen zur Förderung globaler Lösungen zu suchen. Indem sie die Erfahrungen der europäischen Länder in die weltweite Debatte mit einbringt, ermutigt die Konferenz zu einem Geist der Zusammenarbeit, der vollständig mit der Förderung der Grundrechte und Freiheiten im Einklang steht.

Mit dieser Erklärung nimmt die Konferenz zur Kenntnis, dass sich die Datenschutzlandschaft sowohl innerhalb als auch außerhalb Europas weiterentwickelt. Sie sieht auch die Notwendigkeit, unsere Arbeit zur Förderung des Datenschutzes und der Datenschutzstandards fortzusetzen, indem wir uns an die Welt anpassen, in der wir leben.

Anlage 33

Europäische Datenschutzkonferenz am 23./24. April 2009 in Edinburgh

Entschließung zu bilateralen und multilateralen Abkommen zwischen europäischen Staaten und Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Datenschutzstandards in bilateralen und multilateralen Abkommen, die europäische Staaten mit Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit geschlossen haben, weisen große Unterschiede auf.

Die geltenden Rechtsrahmen, die Konvention 108, ihre Protokolle und der Rahmenbeschluss 2008/977/JHA über den Schutz personenbezogener Daten gewährleisten ein besonderes datenschutzrechtliches Regelwerk für den Austausch personenbezogener Daten.

Angesichts dieser Tatsache weist die Europäische Datenschutzkonferenz darauf hin, dass diese großen Unterschiede das von den europäischen Staaten verfolgte Ziel, nämlich die Schaffung eines möglichst einheitlichen und effektiven Datenschutzes für alle Personen, gefährden.

Die Konferenz fordert daher alle europäischen Staaten auf, sicherzustellen, dass beim Abschluss internationaler Abkommen geltende Datenschutzstandards eingehalten werden. In diesem Zusammenhang setzt sich die Konferenz nachdrücklich für die Entwicklung und die anschließende Aufnahme solcher datenschutzrechtlicher Standardklauseln in diesen Abkommen ein.

Anlage 34

Europäische Datenschutzkonferenz am 29./30. April 2010 in Prag

Entschließung zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf der Grundlage des Abschlussberichts der sogenannten High Level Contact Group wollen Vertreter der Europäischen Union und der Vereinigten Staaten von Amerika Verhandlungen über ein Abkommen zu Datenschutzstandards für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aufnehmen.

Die Europäischen Datenschutzbeauftragten begrüßen dieses Vorhaben sehr. Sie hegen große Hoffnung, dass sich die Europäische Union und die Vereinigten Staaten von Amerika durch dieses Abkommen verpflichten werden, beim Austausch personenbezogener Daten in Strafsachen ein hohes Datenschutzniveau einzuhalten und dadurch ein Beispiel für andere internationale Abkommen zum Datenaustausch im Bereich der Strafverfolgung geben.

Die europäischen Datenschutzbeauftragten messen dem Abkommen große Bedeutung bei, denn angesichts von internationalem Terrorismus und grenzüberschreitender Kriminalität werden die Herausforderungen an die internationale Kooperation von Strafverfolgungsbehörden aller Voraussicht nach weiter anwachsen und damit auch die Bedingungen für den internationalen Datenaustausch zwischen den Sicherheitsbehörden zunehmend auf der politischen Tagesordnung stehen.

In diesem Sinne fordert die Europäische Datenschutzkonferenz die Europäische Union auf, sich für ein hohes Datenschutzniveau stark zu machen und – mittels dieses Abkommens – unverrückbare Prinzipien – insbesondere eine enge Zweckbindung der übermittelten Daten, eine hohe Datensicherheit, unabhängige Datenschutzaufsichtsbehörden sowie das Auskunftsrecht und den gerichtlichen Rechtsschutz für alle Betroffenen, unabhängig von ihrer Nationalität oder ihres Aufenthaltslandes – auch bei einem Datenaustausch mit den USA auf effektive Weise sicherzustellen.

Nähere Einzelheiten zu den Erwartungen und Hoffnungen der Europäischen Datenschutzkonferenz finden Sie in dem gemeinsamen Beitrag der WPPJ und der Artikel 29-Arbeitsgruppe zu der öffentlichen Konsultation der Europäischen Kommission in dieser Angelegenheit.

Anlage 35

Europäische Datenschutzkonferenz am 29./30. April 2010 in Prag

Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen

Der gescheiterte Anschlag auf den Delta Flug 253 Amsterdam – Detroit am 25. Dezember 2009 entfachte eine weltweite Diskussion bei Regierungen und Sicherheitsbehörden darüber, wie die Sicherheit auf Flughäfen erhöht werden könnte und ob Körperscanner zur Erleichterung der Kontrollen der Flugpassagiere, bevor sie an Bord gehen, eingesetzt werden sollten. Der Einsatz solcher Körperscanner und das Durchleuchten des gesamten menschlichen Körpers kann eine schwere Verletzung des Rechts des Passagiers auf Schutz der Privatsphäre und auf Datenschutz darstellen. Daher sollten Datenschutzprinzipien und -sicherungsmaßnahmen ebenso berücksichtigt werden wie „Privacy by Design“, wenn der Einsatz von Körperscannern in Erwägung gezogen wird.

Die Notwendigkeit der Verarbeitung ist eines der Datenschutzprinzipien, das berücksichtigt werden muss. Es ist immer noch nicht klar, ob sich mit diesen Geräten wirklich eine höhere Sicherheit an Flughäfen erreichen lässt. Vor ihrem Einsatz muss auch die Frage hinsichtlich ihrer Effektivität und ihrer Auswirkungen auf die Gesundheit der Passagiere in Betracht gezogen werden.

Vor dem Hintergrund des aktuellen Diskussionsstandes sieht die Europäische Datenschutzkonferenz mit Besorgnis, dass neue Geräte eingesetzt werden, die nicht den Datenschutzstandards entsprechen. Deshalb möchte die Konferenz die Notwendigkeit einer wissenschaftlich fundierten und koordinierten Diskussion dieses Themas betonen.[1] Alle Interessengruppen wie Wissenschaftler, Technikexperten, Fachleute aus den Bereichen Gesundheit und Datenschutz sollten angehört werden, um zu einer angemessenen Bewertung der anstehenden Punkte zu gelangen. Insbesondere sind vor einer voreiligen Entscheidung zu dem Einsatz von Körperscannern die folgenden Aspekte anzusprechen.

1. Ist der Einsatz von Körperscannern an Flughäfen für die Flugsicherheit notwendig und wenn ja, in welchen Ausmaß? Zu dieser Frage sind detaillierte Studien unter Einbeziehung wissenschaftlicher Methoden durchzuführen. Die Nützlichkeit der Körperscanner sollte auf einer soliden empirischen Grundlage bewiesen werden. Bis heute gibt es ernsthafte Zweifel hinsichtlich der erweiterten Fähigkeiten der Körperscanner mit Blick auf die Detektierbarkeit explosiver Stoffe, wie zum Beispiel kleiner Mengen von Flüssigkeiten oder anderer Stoffen von geringer Dichte. Ist im Vergleich mit anderen Methoden zur Personenkontrolle wie dem Gang durch Metalldetektoren, Handscannern oder

[1] Die Art. 29 WP hat am 11. Februar 2009 ein Arbeitspapier zu Körperscannern angenommen. Dieses Arbeitspapier und der Begleitbrief an die Europäische Kommission sind auf folgenden Webseiten zu finden:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_annex_consultation_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

Leibesvisitationen ein Zugewinn an Sicherheit zu verzeichnen? Falls es weniger einschneidende Methoden zur Erreichung des gleichen zusätzlichen Sicherheitsniveaus gibt,[2] dann sollten diese genutzt werden.

2. Gibt es angemessene Schutzmaßnahmen, die die Privatsphäre der durch Körperscanner durchleuchteten Personen gewährleisten? Technische Maßnahmen müssen sicherstellen, dass die personenbezogenen Daten der Reisenden weder gespeichert noch weitergeleitet werden. Sobald der Passagier für sicher erklärt wurde, sollten die Bilder sofort gelöscht werden. Schematische Darstellungen der Körper von Personen sind überaus datenschutzfreundlich. Daher könnte dieser Methode, Körper auf Bildschirmen zu zeigen, der Vorzug gegeben werden. Falls intime Details von Personen, wie z. B. medizinische Hilfsmittel oder künstliche Körperteile angezeigt werden, sollten sie nur für die diensthabende Person zu sehen sein. Die mit dem Ansehen der vom Körperscanner angezeigten Bilder befassten Personen dürfen nicht mit den Personen, die an weiteren Kontrollen beteiligt sind, identisch sein. Sie müssen ihre Aufgaben in Einrichtungen wahrnehmen, die ihnen keine Kommunikation mit den anderen Kontrolleuren erlauben, und sie dürfen nicht in der Lage sein, die Passagiere zu sehen. Außerdem sollten Körperscanner nur eingesetzt werden, nachdem eine Datenschutz-Verträglichkeitsprüfung (PIA) durchgeführt wurde, aus der hervorgehen sollte, dass die hier erwähnten Grundsätze mit einbezogen wurden.

Nur wenn ein fairer Ausgleich zwischen der Effektivität und Notwendigkeit dieser neuen technologischen Geräte einerseits und der Auswirkung auf die Privatsphäre der Flugpassagiere andererseits geschaffen wird, könnte der Einsatz von Körperscannern aus datenschutzrechtlicher Sicht als angemessen und als ein geeignetes Mittel für die Sicherheitsdurchleuchtung betrachtet werden.

Deshalb ruft die Europäische Datenschutzkonferenz alle Entscheidungsträger aus ganz Europa dazu auf, gründlich über die Auswirkungen der Körperscanner auf die Grundrechte der Reisenden nachzudenken, bevor sie ihren Einsatz am Flughafen beschließen.

Es sollten nur Geräte eingesetzt werden, in die datenschutzfreundliche Technologien eingebaut wurden und die einen angemessenen Ausgleich zwischen der Notwendigkeit nach erhöhter Sicherheit und dem Recht auf Schutz der Privatsphäre und des Datenschutzes schaffen. Die Datenschutzbehörden sollten weiterhin in den Entscheidungsprozess einbezogen werden, insbesondere während der Probe- und Testphasen, vor allem durch Vorabprüfung von Körperscannersystemen (falls nach nationalem Recht anwendbar) und durch Kontrollmöglichkeiten mit Blick auf das Funktionieren der Geräte nach deren Installation.

Die Passagiere sollten vor der Kontrolle durch Körperscanner angemessen über diese Geräte und über ihre Datenschutzrechte informiert werden. Zu diesem Zweck sollten die Flughafenbehörden eng mit ihren jeweils zuständigen Datenschutzbehörden zusammenarbeiten um sicherzustellen, dass entsprechende Merkblätter den rechtlichen Anforderungen entsprechen.

---

[2] wie z. B. Handscanner oder Spürhunde

Anlage 36

Europäische Datenschutzkonferenz am 5. April 2011 in Brüssel

Entschließung über die Notwendigkeit eines umfassenden Rechtsrahmens für den Datenschutz

Die europäischen Datenschutzbehörden hatten bereits auf Ihrer Frühjahrskonferenz in Edinburgh[1] im Jahr 2009 eine Erklärung angenommen, in der sie ihre Absicht ausdrückten, einen aktiven Beitrag zur Debatte zu leisten und für die Notwendigkeit eines hohen Datenschutzstandards in allen Lebensbereichen, einschließlich der Entwicklung von Technologien, der Online-Welt und Strafverfolgungsmaßnahmen, zu werben.

Diese Erklärung zur Führungsrolle wurde auf der Frühjahrskonferenz in Prag im Jahr 2010[2] bestätigt. Die Datenschutzbeauftragten betonten vor allem die Notwendigkeit, eine wirksame und konsequente Umsetzung der Grundrechte in einem globalen Umfeld sicherzustellen.

Die Frühjahrskonferenz in Brüssel begrüßt und unterstützt nachdrücklich, dass die Europäische Kommission nun einen ersten konkreten Schritt in Richtung eines umfassenden Datenschutzkonzepts in der Europäischen Union durch die Annahme der Mitteilung 2010 (609) am 4. November 2010 unternommen hat.

Hinsichtlich der Absicht der Kommission, im Laufe des Jahres 2011 einen Vorschlag für einen neuen Rechtsrahmen anzunehmen

- erinnert die Konferenz an die wichtigsten Herausforderungen, die in dem neuen Rechtsrahmen behandelt werden sollen, dazu gehören

    - die Folgen der Globalisierung und des grenzüberschreitenden Verkehrs personenbezogener Daten;

    - die Entwicklung der Technologie, insbesondere in der Online-Welt;

    - die Bedeutung eines wirksamen Schutzes in den Bereichen Polizei und Justiz, auch im Hinblick auf die Tendenz zur systematischen Wiederverwendung personenbezogener Daten des privaten Sektors zu Strafverfolgungszwecken.

- Die Konferenz betont, dass Artikel 8 Absatz 1 der Charta der Grundrechte und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union bestätigen, dass "jeder das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat", unabhängig von der Person oder der Situation.

---

[1] Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa, angenommen von der Europäischen Datenschutzkonferenz am 23.-24. April 2009 in Edinburgh.

[2] Entschließung über die zukünftige Entwicklung des Datenschutzes, angenommen von der Europäischen Datenschutzkonferenz am 30. April 2010 in Prag.

- Die Konferenz stellt fest, dass der neue rechtliche Rahmen mit dem Vertrag von Lissabon und der Grundrechte-Charta den Datenschutz ausdrücklich als ein Grundrecht anerkennt und diesem Recht auch Verbindlichkeit verleiht. Der Vertrag von Lissabon schafft die Pfeilerstruktur ab, die die Ursache eines zersplitterten datenschutzrechtlichen Rahmens auf EU-Ebene war.

- Die Konferenz begrüßt es, dass die Kommission ein "umfassendes Konzept" für den neuen Rechtsrahmen, einschließlich des Bereichs der Strafverfolgung, vorsieht.

- Die Konferenz erkennt an, dass spezifische zusätzliche Vorschriften für bestimmte Bereiche erforderlich sein könnten – einschließlich des Bereichs der Strafverfolgung, so wie es in Erklärung 21 im Anhang zum Vertrag dargelegt wurde, und für andere spezifische Bereiche, wie es bereits für die e-Privacy-Richtlinie der Fall war – die Konferenz besteht jedoch darauf, dass diese bereichsspezifischen zusätzlichen Vorschriften auf keinen Fall das Datenschutzniveau herabsetzen dürfen und dass sie nur rechtmäßige Einschränkungen erlauben sollen, die im Einklang mit den allgemeinen Grundsätzen des Datenschutzes stehen.

Die Konferenz weist nachdrücklich auf die Notwendigkeit eines konsequenten und umfassenden Konzeptes hin, das nicht nur den EU-Rahmen, sondern auch den internationalen Zusammenhang und die Notwendigkeit globaler Standards für den Schutz personenbezogener Daten berücksichtigt. Sie interessiert sich deshalb insbesondere für:

- Die derzeit im Rahmen des Europarats und der OECD laufende Arbeit. Beide Einrichtungen ergreifen wertvolle Initiativen zur Überarbeitung ihrer aktuellen Rechtsrahmen und zur Feststellung der zu modernisierenden Bereiche.

- Die Initiative des Europarats, Nichtvertragsparteien des Übereinkommens Nr. 108 und seines Zusatzprotokolls – unabhängig davon, ob sie Ratsmitglieder sind – zum Beitritt zu diesen Instrumenten zu ermutigen.

- Weitere Initiativen für die Entwicklung internationaler Standards[3], die weltweit anerkannt werden sollen.

Die Konferenz ist der Auffassung, dass Bestrebungen zur Modernisierung und Verstärkung der unterschiedlichen Rechtsrahmen sich in Synergie entwickeln sollen und fordert die Hauptakteure dieser Projekte zur Koordination ihrer Tätigkeiten auf.

Die Datenschutzbeauftragten sind der Auffassung, dass all diese Entwicklungen enorme Chancen für eine wirkliche Verbesserung des Rahmens für den Datenschutz bieten, indem sie allen Betroffenen unter allen Umständen nicht nur jetzt, sondern auch in einer ferneren Zukunft einen wirksamen Datenschutz bieten.

---

[3] Siehe insbesondere:

- Internationale Standards zum Schutz der Privatsphäre, angenommen von der 31. Internationalen Konferenz der Datenschutzbeauftragten am 5. November 2009 in Madrid.

- Entschließung über die Organisation einer internationalen Konferenz zur Entwicklung bindender internationaler Instrumente für den Datenschutz, angenommen von der 32. Internationalen Konferenz der Datenschutzbeauftragten am 29. Oktober 2010 in Jerusalem.

Die Zeit ist gekommen, ehrgeizig zu sein und mit vereinten Kräften auf einen effektiveren Datenschutz hinzuarbeiten. Die Datenschutzbeauftragten sind gerne bereit, alle möglichen Beiträge zu leisten, um so ein starkes und umfassendes Datenschutzregime Realität werden zu lassen.

Anlage 37

31. Internationale Konferenz der Datenschutzbeauftragten vom 4.- 6. November 2009 in Madrid

Entschließung über internationale Standards zum Schutz der Privatsphäre

– Übersetzung –

Berücksichtigend, dass:

- die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Straßburg einstimmig den Beschluss über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Richtlinien zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten fasste;

- die Konferenz die “Agencia Española de Protección de Datos” (im Folgenden: die spanische Datenschutzbehörde, d. Übers.) in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz damit beauftragte, eine Arbeitsgruppe, die sich aus den interessierten Datenschutzbehörden zusammensetzen sollte, mit dem Ziel zu bilden, einen Gemeinsamen Vorschlag zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten auszuarbeiten;

- die spanische Datenschutzbehörde gemäß diesem Auftrag eine Arbeitsgruppe bildete und die Arbeiten zur Erstellung eines Gemeinsamen Vorschlags für die Abfassung internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten förderte und koordinierte;

- die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten insbesondere auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards und Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren, entwickelte;

- bei der Erarbeitung des Gemeinsamen Vorschlags davon ausgegangen wurde, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen könnten und dass die Arbeitsgruppe die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards anstrebte, die trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre als anwendbar betrachtet wurden.

Im Einklang damit beschließt die Konferenz Folgendes:

1. Sie begrüßt den Gemeinsamen Vorschlag zur Abfassung der internationalen Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von personenbezogenen Daten, die diesem Beschluss als Anlage beiliegt. Der Gemeinsame Vorschlag belegt zum angemessenen Zeitpunkt die Möglichkeit der Festlegung solcher

Standards als einen neuen Schritt in Richtung auf die Ausarbeitung eines international verbindlichen Instruments.

2. Sie bestätigt, dass der Gemeinsame Vorschlag Grundsätze, Rechte, Verpflichtungen und Verfahrensweisen enthält, die zum Datenschutz und zum Schutz der Privatsphäre von allen Rechtssystemen angestrebt werden sollten. Auf diese Weise könnte die Verarbeitung personenbezogener Daten im öffentlichen und privaten Sektor weltweit einheitlicher erfolgen, und zwar:

a) fair, rechtmäßig und angemessen im Hinblick auf bestimmte explizite und legitime Zwecke;

b) auf der Grundlage einer transparenten Politik, mit angemessenen Informationen für die Interessierten und ohne willkürliche Diskriminierungen, die diesen Grundsätzen widersprächen;

c) die Genauigkeit, Vertraulichkeit und Sicherheit der Daten sowie die Legitimität der Datenverarbeitung und die Rechte der Betroffenen auf Einsehen, Richtigstellung und Löschung der Daten sowie auf Widerspruch gegen eine bestimmte Datenverarbeitung gewährleistend;

d) unter Anwendung des Haftungsprinzips, einschließlich der Schadenshaftung, was auch die Datenverarbeitung durch Dienstleistungserbringer, die im Auftrag des Verantwortlichen handeln, einschließt;

e) mit geeigneteren Garantien, wenn es sich um sensible Daten handelt;

f) mit der Gewährleistung, dass international übertragene Daten unter dem in den genannten Standards vorgesehenen Schutz stehen;

g) indem die Datenverarbeitung unter die Kontrolle von unabhängigen und unparteiischen Aufsichtsbehörden gestellt wird, die über die angemessenen Befugnisse und Ressourcen verfügen müssen und zur Zusammenarbeit verpflichtet sind;

h) durch die Schaffung eines neuen und modernen Bezugsrahmens proaktiver Maßnahmen, deren Ziel insbesondere die Vorbeugung und Feststellung von Verstößen ist und die auf der Ernennung von Beauftragten für den Datenschutz und den Schutz der Privatsphäre, wirksamen Audits und Datenschutz-Folgenabschätzungen beruhen.

3. Sie ermutigt die bei der Internationalen Konferenz akkreditierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre zur Verbreitung des Gemeinsamen Vorschlags zur Abfassung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten.

4. Sie beauftragt die für die Organisation der 31. und 32. Internationalen Konferenzen Verantwortlichen mit dem Aufbau einer Kontaktgruppe, an der die interessierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre teilnehmen sollen. Diese Gruppe soll folgende Aufgaben in Angriff nehmen:

a) Die Förderung und die Verbreitung des Gemeinsamen Vorschlags unter privaten Instanzen, Experten sowie in- und ausländischen öffentlichen Stellen, insbesondere unter den in der Erklärung von Montreux aufgeführten Institutionen und Or-

ganisationen als Grundlage für die zukünftige Arbeit an einem verbindlichen universellen Abkommen; sowie

b) die Untersuchung und Information über weitere Möglichkeiten der Verwendung des Gemeinsamen Vorschlags als Grundlage für die Entwicklung eines weltweiten Verständnisses und einer internationalen Kooperation im Bereich des Datenschutzes und des Schutzes der Privatsphäre, insbesondere im Kontext der internationalen Übertragung personenbezogener Daten, bei der die Rechte und Freiheiten der Individuen geschützt werden müssen.

5. Die Kontaktgruppe soll:

a) ihre Arbeit mit der Steuerungsgruppe der Konferenz koordinieren und über ihre Vertretung auf Sitzungen internationaler Organisationen entscheiden, sowie

b) die 32. Internationale Konferenz über ihre Fortschritte informieren, damit die Aufmerksamkeit dauerhaft auf das Thema des vorliegenden Beschlusses gerichtet wird.

Erläuterung

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre fasste in Straßburg einstimmig die Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten. Diese wurde gemeinsam von den Datenschutzbehörden der Schweiz und Spaniens vorgelegt und von zwanzig weiteren Behörden unterstützt.

In dieser Entschließung erinnert die Konferenz daran, dass diverse Erklärungen und Beschlüsse in den letzten zehn Jahren darauf abzielten, den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre zu stärken und zur Erstellung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten aufzurufen.

Außerdem betont der Beschluss, dass die Internationale Konferenz der Ansicht ist, das Recht auf Datenschutz und den Schutz der Privatsphäre sei ein Grundrecht der Menschen, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz. Gleichzeitig stellt sie fest, dass die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden.

Deshalb wird in dem Beschluss die Überzeugung der Konferenz zum Ausdruck gebracht, dass die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt.

In diesem Sinne unterstützt der Beschluss der Internationalen Konferenz die Anstrengungen des Europarats, die Grundrechte auf den Datenschutz und den Schutz der Privatsphäre zu fördern und sie fordert die Staaten – unabhängig davon, ob sie Mitglieder

dieser Organisation sind oder nicht – auf, das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und das Zusatzprotokoll zu ratifizieren. Gleichzeitig unterstützt die Konferenz die Initiativen der APEC, der OECD sowie anderer regionaler Organisationen und internationaler Foren, wirksame Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre zu entwickeln.

Die Konferenz beauftragte die spanische Datenschutzbehörde in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz, eine Arbeitsgruppe zu bilden, die sich aus den interessierten Datenschutzbehörden zusammensetzen soll, und deren Ziel es ist, einen Gemeinsamen Vorschlag zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten zu entwickeln.

Der Beschluss enthält eine Reihe von Kriterien, die den Prozess zur Ausarbeitung dieses gemeinsamen Vorschlags lenken, insbesondere, dass öffentliche und private Organisationen und Instanzen zu einer breiten Beteiligung ermutigt werden sollen, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen.

Gemäß diesem Auftrag bildete die spanische Datenschutzbehörde die Arbeitsgruppe, auf die sich der Beschluss bezieht, und förderte und koordinierte die Arbeiten zur Erstellung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards. Die spanische Datenschutzbehörde lud alle bei der Internationalen Konferenz akkreditierten Behörden für den Datenschutz und den Schutz der Privatsphäre zur Teilnahme ein. Die im Anhang II aufgeführten Instanzen bekundeten ihren Willen, an dieser Arbeitsgruppe teilzunehmen und versammelten sich daraufhin.

Die Arbeitsgruppe kam im Januar und Juni 2009 zusammen. Auf der ersten Sitzung wurde die Vorgehensweise zur Abfassung des Gemeinsamen Vorschlags und dessen inhaltliche Reichweite beschlossen und auf der zweiten Sitzung wurde eine fortgeschrittene Entwurfsversion besprochen, die später an die 31. Internationale Konferenz weitergeleitet werden sollte.

Die spanische Datenschutzbehörde leistete auf der Grundlage des Straßburger Beschlusses und der in der Arbeitsgruppe festgelegten Kriterien und Arbeitsmethoden eine gründliche Arbeit: Es wurde eine Reihe von Arbeitspapieren verfasst, an deren Ausarbeitung Beauftragte für den Datenschutz und den Schutz der Privatsphäre und andere mit dem Datenschutz verbundene öffentliche Instanzen sowie Experten aus privaten Unternehmen, Juristen, Wissenschaftler sowie internationale Organisationen und Nicht-Regierungs-Organisationen beteiligt waren.

Insbesondere entwickelte die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards oder Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren. Bei der Erarbeitung des Gemeinsamen Vorschlags wurde davon ausgegangen, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen. Ziel der Arbeitsgruppe war die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards, die aber trotz der bestehenden

Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre anwendbar sind.

Anlage

Gemeinsamer Vorschlag zur Erstellung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten

Teil I: Allgemeine Bestimmungen

1. Ziel

Das Ziel des vorliegenden Dokuments ist:

1. Die Definition einer Reihe von Grundsätzen und Rechten, die den tatsächlichen und einheitlichen Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten weltweit garantieren; und

2. die Erleichterung des internationalen Flusses von personenbezogenen Daten – das ist eine Notwendigkeit in einer globalisierten Welt.

2. Definitionen

Das vorliegende Dokument versteht unter:

a) „Personenbezogenen Daten“: Jegliche Information bezüglich einer identifizierten natürlichen Person bzw. einer natürlichen Person, die mit den vernünftigerweise einzusetzenden Mitteln identifiziert werden kann.

b) „Verarbeitung“: Jeglicher Vorgang oder eine Reihe von Vorgängen, die automatisiert sein können oder nicht, und die auf personenbezogene Daten angewendet werden, das betrifft insbesondere deren Erhebung, Aufbewahrung, Enthüllung oder Löschung.

c) „Betroffener“: Eine natürliche Person, deren personenbezogene Daten verarbeitet werden.

d) „Verantwortliche Person“: Eine natürliche oder juristische Person, öffentlich oder privat, die allein oder in Zusammenarbeit mit anderen über die Verarbeitung entscheidet.

e) „Dienstleistungserbringer“: Eine natürliche oder juristische Person, die nicht die verantwortliche Person ist und die personenbezogenen Daten im Auftrag der besagten verantwortlichen Person verarbeitet.

3. Anwendungsbereich

1. Das vorliegende Dokument gilt für jegliche Verarbeitung personenbezogener Daten, die voll- oder teilautomatisch oder andernfalls in strukturierter Form im öffentlichen oder im privaten Sektor vollzogen wird.

2. Die jeweilige nationale Gesetzgebung kann festlegen, dass die Bestimmungen des vorliegenden Dokuments nicht auf die Verarbeitung personenbezogener Daten anzu-

wenden sind, wenn diese von einer natürlichen Person im Rahmen von ausschließlich privaten bzw. familiären Tätigkeiten ausgeführt wird.

4. Zusätzliche Maßnahmen

1. Die Staaten können das in dem vorliegenden Dokument definierte Schutzniveau um zusätzliche Maßnahmen, die einen besseren Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten garantieren, ergänzen.

2. Die Bestimmungen des vorliegenden Dokuments bilden eine geeignete Grundlage für die grenzüberschreitende Übermittlung personenbezogener Daten, wenn dies gemäß den Vorgaben des Artikels 15 des vorliegenden Dokuments geschieht.

5. Ausnahmen

Die Staaten können die Reichweite der in den Artikeln 7 bis 10 und 16 bis 18 enthaltenen Bestimmungen einschränken, wenn dies in einer demokratischen Gesellschaft notwendig ist, um die nationale Sicherheit, die öffentliche Sicherheit, den Schutz der öffentlichen Gesundheit oder den Schutz der Rechte und Freiheiten anderer zu gewährleisten. Solche Einschränkungen müssen im nationalen Recht ausdrücklich vorgesehen sein, das heißt, ihre Grenzen müssen festgelegt werden und es muss angemessene Garantien zum Schutz der Rechte der Betroffenen geben.

Teil II: Grundlegende Prinzipien

6. Prinzipien der Rechtmäßigkeit und Fairness

1. Die Verarbeitung personenbezogener Daten muss fair ausgeführt werden, wobei die anwendbare nationale Gesetzgebung sowie die Rechte und Freiheiten der Menschen im Einklang mit den Inhalten des vorliegenden Dokuments und den Zielen und Grundsätzen der Allgemeinen Erklärung der Menschenrechte und dem Internationalen Pakt über bürgerliche und politische Recht eingehalten werden müssen.

2. Insbesondere eine Verarbeitung personenbezogener Daten, die eine ungerechte oder willkürliche Diskriminierung der Betroffenen darstellt, wird als unredlich angesehen.

7. Prinzip der Zweckgebundenheit

1. Die Verarbeitung personenbezogener Daten muss sich auf die Erfüllung bestimmter, expliziter und legitimer Zwecke, die die verantwortliche Person verfolgt, beschränken.

2. Die verantwortliche Person darf keine Verarbeitungen durchführen, die nicht den Zwecken, für die die personenbezogenen Daten erhoben wurden, entsprechen, außer sie verfügt über das eindeutige Einverständnis des Betroffenen.

8. Verhältnismäßigkeitsprinzip

1. Die Verarbeitung der personenbezogenen Daten muss sich auf solche beschränken, die für die im vorherigen Absatz beschriebenen Zwecke angemessen, relevant und nicht exzessiv sind.

2. Insbesondere muss die verantwortliche Person angemessene Anstrengungen leisten, um die verarbeiteten personenbezogenen Daten auf ein notwendiges Mindestmaß zu reduzieren.

9. Qualitätsprinzip

1. Die verantwortliche Person muss jederzeit sicherstellen, dass die personenbezogenen Daten exakt sind und dass sie so vollständig und aktuell gehalten werden, wie es für die Erfüllung der Zwecke, für die sie verarbeitet werden, notwendig ist.

2. Die verantwortliche Person muss die Aufbewahrungszeit der verarbeiteten personenbezogenen Daten auf die erforderliche Mindestzeit beschränken. Wenn also die personenbezogenen Daten für die Erfüllung der Zwecke, die ihre Verarbeitung legitimierten, nicht mehr notwendig sind, müssen sie gelöscht oder anonymisiert werden.

10. Transparenzprinzip

1. Jede verantwortliche Person muss die von ihr durchgeführte Verarbeitung personenbezogener Daten in einer Datenschutzerklärung transparent machen.

2. Die verantwortliche Person muss dem Betroffenen zumindest über ihre Identität, den Zweck, zu dem sie die Verarbeitung auszuführen beabsichtigt, die Adressaten, an die sie die personenbezogenen Daten weiterzuleiten gedenkt und die Art, auf die der Betroffene seine in dem vorliegenden Dokument beschriebenen Rechte ausüben können, sowie alle weiteren Informationen, die die loyale Verarbeitung dieser personenbezogenen Daten gewährleistet, informieren.

3. Wenn die personenbezogenen Daten direkt von dem Betroffenen geliefert wurden, muss die Information zum Zeitpunkt der Datenerhebung gegeben werden, falls sie nicht schon vorher erteilt wurde.

4. Falls die personenbezogenen Daten nicht direkt vom Betroffenen stammen, muss die Information innerhalb eines angemessenen Zeitraums erbracht werden, obwohl sie auch durch alternative Maßnahmen ersetzt werden kann, falls die Erfüllung dieser Vorgabe unmöglich ist oder von der verantwortlichen Person einen unverhältnismäßigen Aufwand verlangt.

5. Alle Informationen, die dem Betroffenen gegeben werden, müssen verständlich und in einer eindeutigen und einfachen Sprache abgefasst sein, was insbesondere für solche Verarbeitungen gilt, die sich speziell an Minderjährige richten.

6. Wenn die personenbezogenen Daten online über elektronische Kommunikationsnetze erhoben werden, können die in diesem Artikel enthaltenen Verpflichtungen erfüllt werden, indem die Datenschutzpolitik leicht zugänglich und erkennbar veröffentlicht wird, wobei alle oben aufgeführten Punkte eingehalten werden müssen.

11. Verantwortlichkeitsprinzip

Die verantwortliche Person muss:

a) Die notwendigen Maßnahmen zur Erfüllung der in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung aufgeführten Grundsätze und Verpflichtungen ergreifen; und

b) die erforderlichen Nachweise über die Erfüllung der o. g. Vorgaben erbringen, und zwar sowohl gegenüber dem Betroffenen als auch gemäß Artikel 23 gegenüber den zuständigen Aufsichtsbehörden.

Teil III: Rechtfertigung der Verarbeitung

12. Allgemeines Rechtfertigungsprinzip

1. Als allgemeine Regel gilt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn einer der folgenden Punkte erfüllt wird:

a) nach Erhalt des freien, eindeutigen und informierten Einverständnisses des Betroffenen;

b) wenn ein legitimes Interesse der verantwortlichen Person die Verarbeitung rechtfertigt, vorausgesetzt, dass die legitimen Interessen, Rechte oder Freiheiten des Betroffenen keinen Vorrang haben;

c) wenn die Verarbeitung für die Aufrechterhaltung oder Erfüllung eines Rechtsverhältnisses zwischen der verantwortlichen Person und dem Betroffenen erforderlich ist;

d) wenn die Verarbeitung für die Erfüllung einer Verpflichtung, die der verantwortlichen Person von der anzuwendenden nationalen Gesetzgebung auferlegt wird, notwendig ist oder wenn sie von einer öffentlichen Behörde, die diese für die legitime Erfüllung ihrer Zuständigkeiten benötigt, ausgeführt wird;

e) wenn außergewöhnliche Umstände auftreten, die das Leben, die Gesundheit oder die Sicherheit des Betroffenen oder einer anderen Person gefährden.

2. Die verantwortliche Person muss den Betroffenen einfache, schnelle und wirksame Verfahren bereitstellen, damit diese ihr Einverständnis jederzeit zurücknehmen können. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für die Betroffenen noch Einkünfte der verantwortlichen Person verursachen.

13. Sensitive Daten

1. Als sensitiv werden folgende personenbezogenen Daten betrachtet:

a) Solche, die die Intimsphäre des Interessierten betreffen; oder

b) wenn deren ungerechtfertigte Verwendung

i. eine gesetzwidrige oder willkürliche Diskriminierung verursacht; oder

ii. ein schwerwiegendes Risiko für den Betroffenen darstellt.

2. Insbesondere werden solche personenbezogenen Daten als sensibel eingestuft, die Aufschluss über Aspekte wie die rassische oder ethnische Herkunft, politische Einstellungen, religiöse oder philosophische Überzeugungen geben, sowie Daten, die sich auf die Gesundheit oder die Sexualität beziehen. Falls die Umstände, auf die der vorhergehende Artikel sich bezieht, auftreten, kann die anzuwendende nationale Gesetzgebung weitere Kategorien für sensitive Daten vorsehen.

3. In der jeweiligen nationalen Gesetzgebung müssen die notwendigen Garantien zum Schutz der Rechte der Betroffenen festgeschrieben werden. Diese müssen zusätzliche Bedingungen für die Verarbeitung sensibler personenbezogener Daten enthalten.

14. Datenverarbeitung im Auftrag

Die verantwortliche Person kann die Verarbeitung von personenbezogenen Daten von verschiedenen Auftragnehmern durchführen lassen. In diesem Fall verpflichtet sie sich zur:

a) Kontrolle, dass jeder Auftragnehmer sicherstellt, dass zumindest das in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung vorgeschriebene Schutzniveau eingehalten wird; und

b) Verbindlichmachung der Rechtsbeziehung mittels eines Vertrags oder eines anderen Rechtsakts, der das Vorhandensein, die Reichweite und den Inhalt des Rechtsverhältnisses nachweist und den Auftragnehmer zur Einhaltung dieser Garantien und zur Gewährleistung, dass die personenbezogenen Daten gemäß der Anweisungen der verantwortlichen Person verarbeitet werden, verpflichtet.

15. Internationaler Datenverkehr

1. Als allgemeine Regel gilt, dass personenbezogene Daten grenzüberschreitend übermittelt werden können, wenn der Staat, in den diese Daten übertragen werden, zumindest das in dem vorliegenden Dokument vorgesehene Schutzniveau bietet.

2. Übermittlungen personenbezogener Daten in Staaten, die das in dem vorliegenden Dokument vorgesehene Schutzniveau nicht bieten, sind möglich, wenn derjenige, der die Daten zu übertragen beabsichtigt, garantiert, dass der Empfänger dieses Schutzniveau sicherstellt. Diese Garantie kann sich beispielsweise aus geeigneten vertraglichen Klauseln ableiten. Insbesondere, wenn die Datenübermittlung im Rahmen multinationaler Organisationen oder Unternehmensgruppen erfolgt, kann diese Garantie durch interne Datenschutzbestimmungen, deren Einhaltung rechtsverbindlich ist, geleistet werden.

3. Wenn die Übermittlung im Rahmen einer Vertragsbeziehung zugunsten des Betroffenen, zum Schutz eines lebenswichtigen Interesses des Betroffenen bzw. einer anderen Person oder zur Erfüllung einer gesetzlichen Verpflichtung zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, kann die für den Datenexporteur geltende nationale Gesetzgebung die Übermittlung der personenbezogenen Daten in Staaten zulassen, die das im vorliegenden Dokument vorgesehene Schutzniveau nicht bieten.

4. Die anzuwendende nationale Gesetzgebung kann die in Artikel 23 genannten Aufsichtsbehörden, die im Absatz 23 vorgesehen sind, zur vorherigen Genehmigung aller oder einiger grenzüberschreitender Übermittlungen von personenbezogenen Daten ermächtigen, die von ihrem Zuständigkeitsbereich aus erfolgen. Auf jeden Fall muss derjenige, der die personenbezogenen Daten ins Ausland übermitteln will, nachweisen, dass die Übermittlung die im vorliegenden Dokument vorgesehenen Garantien erfüllt, insbesondere wenn dies von den Aufsichtsbehörden in Ausübung ihrer im Artikel 23.2 vorgesehenen Zuständigkeiten gefordert wird.

Teil IV: Die Rechte des Betroffenen

16. Recht auf Einsicht

1. Der Betroffene hat das Recht, bei der verantwortlichen Person Informationen über die konkreten, zu verarbeitenden, personenbezogenen Daten sowie über die Herkunft dieser Daten, die Zwecke ihrer Verarbeitung und die Empfänger bzw. Empfängerkategorien zu verlangen, an die diese Daten weitergeleitet werden bzw. werden sollen.

2. Alle Informationen, die dem Betroffenen zugänglich gemacht werden, müssen in einer verständlichen, klaren und einfachen Sprache gehalten sein.

3. Die anzuwendende nationale Gesetzgebung kann die wiederholte Ausübung dieser Rechte, die die verantwortliche Person dazu veranlassen würde in kurzen Zeitabständen eine Vielzahl von Anträgen zu beantworten, einschränken, außer in den Fällen, in denen der Betroffene in seinem Antrag ein berechtigtes Interesse nachweist.

17. Recht auf Berichtigung und Löschung

1. Der Betroffene hat das Recht, bei der verantwortlichen Person die Berichtigung oder Löschung unvollständiger, ungenauer, unnötiger oder übermäßiger personenbezogener Daten zu beantragen.

2. Wenn dieser Fall eintritt, muss die verantwortliche Person die personenbezogenen Daten antragsgemäß berichtigen oder löschen. Er muss dies außerdem den Dritten, an die er die personenbezogenen Daten weitergeleitet hat, mitteilen, falls er diese kennt.

3. Die Löschung erfolgt nicht, wenn die personenbezogenen Daten entsprechend einer der verantwortlichen Person von der nationalen Gesetzgebung auferlegten Verpflichtung oder infolge der Vertragsbeziehungen zwischen der verantwortlichen Person und dem Betroffenen aufbewahrt werden müssen.

18. Widerspruchsrecht

1. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten widersprechen, wenn er einen berechtigten Grund aufgrund seiner konkreten persönlichen Situation vorbringt.

2. Dieses Widerspruchsrecht kann nicht ausgeübt werden, wenn die Verarbeitung der personenbezogenen Daten der verantwortlichen Person von der nationalen Gesetzgebung vorgeschrieben ist.

3. Jeder Betroffene kann gleichfalls solchen Entscheidungen widersprechen, die allein auf der automatischen Verarbeitung der personenbezogenen Daten beruhende Rechtsfolgen nach sich ziehen, es sei denn die Entscheidung wurde von dem Betroffenen ausdrücklich beantragt oder sie ist für den Abschluss, die Aufrechterhaltung oder Erfüllung einer Rechtsbeziehung zwischen der verantwortlichen Person und dem Betroffenen erforderlich. In diesem letzten Fall muss der Betroffene zur Verteidigung seines Rechts oder Interesses die Möglichkeit zur Geltendmachung seiner Sichtweise haben.

19. Ausübung dieser Rechte

1. Die in den Artikeln 16 bis 18 des vorliegenden Dokuments aufgeführten Rechte können folgendermaßen ausgeübt werden:

a) direkt vom Interessierten, der sich gegenüber der verantwortlichen Person angemessen ausweisen muss.

b) über einen Vertreter, der diese Eigenschaft gegenüber der verantwortlichen Person entsprechend nachweisen muss.

2. Die verantwortliche Person muss Verfahren vorsehen, die es den Betroffenen ermöglichen, die in den Absätzen 16 bis 18 des vorliegenden Dokuments vorgesehenen Rechte einfach, schnell und wirksam auszuüben. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für den Betroffenen noch Einkünfte für die verantwortliche Person verursachen.

3. Wenn die verantwortliche Person der Ansicht ist, dass im Einklang mit der anzuwendenden nationalen Gesetzgebung die Ausübung der in diesem Teil aufgeführten Rechte nicht angebracht ist, muss er den Betroffenen vollständig über seine Gründe informieren.

Teil V: Sicherheit

20. Sicherheitsmaßnahmen

1. Sowohl die verantwortliche Person als auch die Auftragnehmer müssen die personenbezogenen Daten, die sie verarbeiten, mit den zu dem jeweiligen Zeitpunkt geeigneten technischen und organisatorischen Mitteln schützen, um ihre Vollständigkeit, Vertraulichkeit und Verfügbarkeit zu gewährleisten. Diese Maßnahmen hängen vom bestehenden Risiko, den möglichen Folgen für die Betroffenen, der Sensitivität der personenbezogenen Daten, dem technischen Zustand und dem Kontext, in dem die Verarbeitung erfolgt, sowie von der jeweiligen nationalen Gesetzgebung ab.

2. Die Betroffenen müssen von denjenigen, die an irgendeiner der Verarbeitungsschritte beteiligt sind, über alle Sicherheitsverstöße, die ihre Vermögens- und Nichtvermögensrechte wesentlich beeinträchtigen könnten, sowie über die ergriffenen Lösungsversuche informiert werden. Diese Information muss früh genug erteilt werden, damit die Betroffenen genügend Zeit haben, zur Verteidigung ihrer Rechte darauf zu reagieren.

21. Datengeheimnis

Die verantwortliche Person und diejenigen, die an irgendeinem der Verarbeitungsschritte der personenbezogenen Daten beteiligt sind, müssen darüber Verschwiegenheit bewahren. Diese Verpflichtung besteht auch dann noch, wenn die Beziehungen mit dem Betroffenen oder der verantwortlichen Person bereits abgeschlossen sind.

Teil VI: Einhaltung und Überwachung

22. Proaktive Maßnahmen

Die Staaten müssen über ihr innerstaatliches Recht Anreize für Maßnahmen schaffen, die eine bessere Einhaltung der Gesetzgebung zum Datenschutz durch diejenigen för-

dern, die an den unterschiedlichen Verarbeitungsschritten beteiligt sind. Zu diesen Maßnahmen können unter anderem Folgende zählen:

a) Die Einführung von Verfahren zur Vorbeugung und Feststellung von Verstößen, die auf standardisierten Modellen zur Steuerung und/oder für das Management der Informationssicherheit beruhen.

b) Die Ernennung eines oder mehrerer Beauftragter für den Schutz der Privatsphäre oder des Datenschutzes, die für die Wahrnehmung ihrer Aufsichtsfunktionen über ausreichende Qualifikationen, Ressourcen und Kompetenzen verfügen müssen.

c) Die regelmäßige Durchführung von Programmen zur Bewusstseinsbildung, Aus- und Weiterbildung der Mitglieder der Organisation zur Verbesserung ihrer Kenntnisse der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren.

d) Die regelmäßige Durchführung von transparenten Audits durch qualifizierte und vorzugsweise unabhängige Personen, bei denen die Einhaltung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren geprüft wird.

e) Die Anpassung der Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, an die auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung, insbesondere wenn es darum geht, Entscheidungen über technische Merkmale, die technische Entwicklung und Implementierung zu treffen.

f) Die Praxisumsetzung von Datenschutz-Folgenabschätzungen vor der Implementierung neuer Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, sowie die Praxisumsetzung neuer Arten der Verarbeitung personenbezogener Daten vor der Einführung wesentlicher Veränderungen der Verarbeitungspraxis.

g) Die Annahme von Verhaltensregeln, deren Einhaltung verpflichtend ist und die es ermöglichen, ihre Wirksamkeit in Bezug auf die Befolgung und den Grad des Schutzes der personenbezogenen Daten zu messen und die wirkungsvolle Maßnahmen im Fall der Nichterfüllung festlegen.

h) Die Einführung von Eventualfallplänen, die Handlungsanweisungen für den Fall festlegen, dass eine Nichtbefolgung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung festgestellt wird, und die zumindest die Verpflichtung enthalten, die Ursache und Reichweite der eingetretenen Vorschriftsverletzung zu bestimmen, ihre negativen Auswirkungen zu beschreiben und die erforderlichen Maßnahmen zu ergreifen, damit das zukünftig nicht noch einmal geschieht.

23. Überwachung

1. In jedem Staat muss es eine oder mehrere Aufsichtsbehörden geben, die im Einklang mit dem innerstaatlichen Recht für die Überwachung der Einhaltung der in dem vorliegenden Dokument festgelegten Grundsätze verantwortlich sind.

2. Diese Aufsichtsbehörden müssen unparteiisch und unabhängig sein und sie müssen über eine angemessene technische Qualifikation, ausreichende Kompetenzen und die geeigneten Ressourcen verfügen, um über die Reklamationen, die die Interessenten an sie richten, entscheiden zu können und um die Untersuchungen und Eingriffe durchführen zu können, die die Befolgung der nationalen Gesetzgebung zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten gewährleisten.

3. Auf jeden Fall und unbeschadet der Einsprüche, die bei den genannten Aufsichtsbehörden eingelegt werden – was auch die gerichtliche Nachprüfung ihrer Entscheidungen einschließt – kann der Betroffene zur Geltendmachung seiner Rechte gemäß den Vorschriften der nationalen Gesetzgebung direkt den Rechtsweg beschreiten.

24. Kooperation und Koordination

1. Die im vorigen Artikel genannten Aufsichtsbehörden müssen bestrebt sein, im Interesse eines einheitlicheren Schutzes der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten sowohl im Inland als auch auf internationaler Ebene miteinander zu kooperieren. Um diese Kooperation zu vereinfachen, müssen die Staaten jederzeit die bei ihnen zuständigen Aufsichtsbehörden benennen können.

2. Diese Behörden bemühen sich insbesondere um die Erfüllung folgender Aufgaben:

a) den Austausch von Studien, Untersuchungsmethoden, Kommunikations- und Regelungsstrategien sowie von allen Informationen, die für eine wirksame Ausübung ihrer Funktionen hilfreich sind, insbesondere nachdem sie von einer anderen Aufsichtsbehörde im Rahmen einer Untersuchung oder Intervention um Unterstützung gebeten worden sind;

b) die Durchführung koordinierter Untersuchungen oder Interventionen – sowohl im Inland als auch auf internationaler Ebene – bei Angelegenheiten, bei denen das Interesse zweier oder mehrerer Aufsichtsbehörden zusammentreffen;

c) die Teilnahme an Verbänden, Arbeitsgruppen oder gemeinsamen Foren sowie Seminaren, Workshops oder Kursen, die dazu beitragen, gemeinsame Standpunkte zu entwickeln oder die technische Qualifizierung des Personals, das diesen Aufsichtsbehörden seine Dienste leistet, zu verbessern;

d) die Aufrechterhaltung einer angemessenen Vertraulichkeit der Informationen, die sie während ihrer Kooperation untereinander ausgetauscht hatten.

3. Die Staaten müssen die Schaffung von Kooperationsvereinbarungen zwischen regionalen, nationalen oder internationalen Aufsichtsbehörden, die zu einer wirksameren Einhaltung dieses Absatzes beitragen, fördern.

25. Haftung

1. Die verantwortliche Person haftet für solche Schäden – sowohl immaterieller als auch materieller Art – die dem Betroffenen durch die Verarbeitung personenbezogener Daten, bei der gegen die Datenschutzvorschriften verstoßen wurde, entstanden sind, es sei denn sie kann nachweisen, dass der Schaden ihr nicht anzulasten ist. Dies gilt unbeschadet des Rechtsanspruchs, den die verantwortliche Person gegenüber den Auftragnehmern, die an den einzelnen Verarbeitungsschritten teilhaben, geltend machen kann.

2. Die Staaten müssen geeignete Maßnahmen fördern, damit die Betroffenen Zugang zu den entsprechenden Gerichts- oder Verwaltungsverfahren haben, die ihnen die Wiedergutmachung der oben erwähnten Schäden ermöglichen.

3. Die in den vorherigen Absätzen vorgesehene Haftung gilt unbeschadet der strafrechtlichen, zivilrechtlichen und verwaltungsrechtlichen Ahndung der Verletzung der Gesetzgebung zum Datenschutz.

4. Das Ergreifen proaktiver Maßnahmen, wie sie im Artikel 22 beschrieben werden, muss bei der Feststellung der Haftung und der Verhängung der in diesem Artikel vorgesehenen Sanktionen berücksichtigt werden.

Anlage 38

SACHSEN-ANHALT

Landesbeauftragter für den Datenschutz

Landesbeauftragter

Herr Dr. von Bose

Leitender Beamter der Geschäftsstelle und Stellvertreter

Herr Cohaus

Dienstgebäude: Leiterstraße 9, 39104 Magdeburg
Postanschrift: Postfach 1947, 39009 Magdeburg
Telefon: 0391 81803-0
Telefax: 0391 81803-33
Freecall: 0800 9153190 (Festnetz DTAG in S.-A.)
E-Mail: poststelle@lfd.sachsen-anhalt.de
Internet: www.datenschutz.sachsen-anhalt.de

Stand: 16. August 2011

Referat 1		**Referat 2**		**Referat 3**
Geschäftsstellenleitung Landtag, Justizverwaltung, Justizvollzug, Staatsanwaltschaften, Europäischer und Internationaler Datenschutz		Grundsatzfragen des Datenschutzrechts, Öffentlicher Dienst, Hochschulen, Kammern	Informationszugangsrecht	Grundsatzfragen der Informationstechnik und der Organisation des Datenschutzes, E-Government, Wirtschaft, Verkehr
Polizei, Verfassungsschutz und Nachrichtendienste	Geschäftsstelle: Haushalts- und Verwaltungsangelegenheiten	Sozialwesen, Verwaltungsverfahrensrecht		IT der Geschäftsstelle, Betriebssysteme, Datenbanken, Netze, Technische Gutachten
Finanzen, Kommunalrecht, Ausländer- und Staatsangehörigkeitsrecht	Geschäftsstelle: Vorzimmer des Landesbeauftragten, Schreibdienst, Bücherei	Gesundheitswesen, Kinder- und Jugendhilfe, Schulen, Wissenschaft und Forschung, Archivwesen, Personalakten- und Personalvertretungsrecht		IT der Geschäftsstelle, Telekommunikations- und Medienrecht, Presserecht, Verwaltungsmodernisierung, E-Government
Melde-, Pass- und Ausweiswesen, Wahlen, Personenstandswesen	Geschäftsstelle: Registratur, Schreibdienst			IT der Geschäftsstelle, Homepage des LfD, Vermessungswesen und Geoinformation, Statistik, Handwerk und Gewerbe

Stichwortverzeichnis

A

B

C

D

E

F

G

P

Q

R

S

T

U

V