LANDTAG RHEINLAND-PFALZ
15. Wahlperiode

Drucksache 15/1764
12. 12. 2007

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Einundzwanzigster Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 2005 bis 30. September 2007

Inhaltsverzeichnis

Dem Präsidenten des Landtags am 12. Dezember 2007 überreicht.
Der Bericht wurde in der Kommission beim Landesbeauftragten für den Datenschutz nach § 26 Abs. 3 Satz 4 Landesdatenschutzgesetz vorberaten.

Druck: Landtag Rheinland-Pfalz, 14. Dezember 2007

I. Anlagenverzeichnis

18. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

19. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Keine heimliche Online-Durchsuchung privater Computer

20. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – GUTE ARBEIT in Europa nur mit gutem Datenschutz

21. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Anonyme Nutzung des Fernsehens erhalten!

22. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

23. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

24. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. Juni 2007 – Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

II. Abkürzungen

ABl.	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
ADD	Aufsichts- und Dienstleistungsdirektion
AG	Arbeitsgruppe
AGs	Arbeitsgemeinschaften
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ArbGG	Arbeitsgerichtsgesetz
Art.	Artikel
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
AuslG	Ausländergesetz
Az.	Aktenzeichen
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BauGB	Baugesetzbuch
BauuntPrüfVO	Bauunterlagenprüfungsverordnung
BDSG	Bundesdatenschutzgesetz
BeamtVG	Beamtenversorgungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BIT	Bundesstelle für Informationstechnik
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMJ	Bundesministerium der Justiz
BMV-Ä	Bundesmantelvertrag-Ärzte
BMV-A/EK	Bundesmantelvertrag-Ärzte/Ersatzkassen
BMWA	Bundesministerium für Wirtschaft und Arbeit
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BSG	Bundessozialgericht
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerwG	Bundesverwaltungsgericht
BVG	Bundesversorgungsgesetz
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
bzgl.	bezüglich
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
ca.	zirka
d.h.	das heißt
DNA	Desoxyribonucleinacid (acid = Säure)
DNA-IFG	DNA-Identitätsfeststellungsgesetz
Drs.	Drucksache
DSO-LT	Datenschutzordnung des Landtags Rheinland-Pfalz
DVBl.	Deutsches Verwaltungsblatt
DVDV	Deutsches Verwaltungsdienste-Verzeichnis
ED	Erkennungsdienst(lich)
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
EGDSRL	Europäische Datenschutzrichtlinie
EGV	Vertrag über die Europäische Gemeinschaft
EHUG	Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EMRK	Europäische Konvention zum Schutz der Menschenrechte und der Grundfreiheiten
EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
evtl.	eventuell
EWOIS	Einwohnerinformationssystem
FahrlG	Fahrlehrergesetz
FeV	Fahrerlaubnis-Verordnung
ff.	(fort-)folgende
FGO	Finanzgerichtsordnung
FM	Ministerium der Finanzen
FRV	Fahrzeugregisterverordnung

G 10	Gesetz zu Artikel 10 GG
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
gem.	gemäß
GemO	Gemeindeordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland
GG	Grundgesetz
ggf.	gegebenenfalls
GOLT	Geschäftsordnung des Landtags Rheinland-Pfalz
GSiG	Gesetz über eine bedarfsorientierte Grundsicherung im Alter und bei Erwerbsminderung
HeilBG	Heilberufsgesetz
IfSG	Infektionsschutzgesetz
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes und der Länder beim Bundeskriminalamt
insbes.	insbesondere
InsO	Insolvenzordnung
INSPIRE	Infrastructure for Spatial Information in Europe
ISM	Ministerium des Innern und für Sport
i.S.v.	im Sinne von
IT	Informationstechnik
i.V.m.	in Verbindung mit
JM	Ministerium der Justiz
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KANN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KDZ	Kommunale Datenzentrale Mainz
KitaG	Kindertagesstättengesetz
KpS	Kriminalpolizeiliche personenbezogene Sammlungen – Kriminalakten –
KRISTAL	kriminalpolizeiliches Recherche- und Informationssystem – Täterorientierte Auswertung, Analyse und Lagedarstellung
KunstUrhG	Kunsturhebergesetz
KV	Kassenärztliche Vereinigung
KWG	Kommunalwahlgesetz
KWO	Kommunalwahlordnung
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LArchG	Landesarchivgesetz
LBauO	Landesbauordnung
LBB	Landesbetrieb Liegenschafts- und Baubetreuung
LBG	Landesbeamtengesetz
LBKG	Landesgesetz über den Brandschutz, die allgemeine Hilfe und den Katastrophenschutz
LDI	Landesbetrieb Daten und Information
LDKN	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LGVerm	Landesgesetz über das amtliche Vermessungswesen
lit.	littera (Buchstabe)
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LKRG	Landeskrebsregistergesetz
LMG	Landesmediengesetz
LPersVG	Landespersonalvertretungsgesetz
LRG	Landesrundfunkgesetz
LSG	Landessozialgericht
LSJV	Landesamt für Soziales, Jugend und Versorgung
LT-Drs.	Landtags-Drucksache
Lufa	Landwirtschaftliche Untersuchungs- und Forschungs-Anstalt Speyer
LV	Landesverfassung für Rheinland-Pfalz
LVA	Landesversicherungsanstalt
LVerfSchG	Landesverfassungsschutzgesetz
LVwVfG	Landesverwaltungsverfahrensgesetz
MASGFF	Ministerium für Arbeit, Soziales, Gesundheit, Familie und Frauen
m.a.W.	mit anderen Worten
MB	Megabyte
MBWJK	Ministerium für Bildung, Wissenschaft, Jugend und Kultur
MDK	Medizinischer Dienst der Krankenversicherung
MEK	Mobiles Einsatzkommando
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
MiStra	Mitteilung in Strafsachen
MinBl.	Ministerialblatt
MMR	Multimedia und Recht
MRRG	Melderechtsrahmengesetz

NJW	Neue Juristische Wochenschrift
NVwZ	Neue Verwaltungszeitschrift
o.ä.	oder ähnliches
OEG	Opferentschädigungsgesetz
OFD	Oberfinanzdirektion
o.g.	oben genanntes
ÖGdG	Landesgesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PassG	Passgesetz
PBefG	Personenbeförderungsgesetz
PC	Personalcomputer
PAuswG	Gesetz über Personalausweise
POG	Polizei- und Ordnungsbehördengesetz
POLADIS	Polizeiliches anwenderorientiertes Daten- und Informationssystem
POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
PostG	Postgesetz
PStG	Personenstandsgesetz
PsychKG	Landesgesetz für psychisch kranke Personen
RdNr.	Randnummer
RDV	Recht der Datenverarbeitung
RGebStV	Rundfunkgebührenstaatsvertrag
RIVAR	Rheinland-pfälzisches Informations-, Vorgangsbearbeitungs-, Auswerte- und Recherchesystem
RSAV	Risikostruktur-Ausgleichsverordnung
s.	siehe
S.	Seite
SchulG	Schulgesetz
SDÜ	Schengener Durchführungs-übereinkommen
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB II	Sozialgesetzbuch – Zweites Buch –
SGB III	Sozialgesetzbuch – Drittes Buch –
SGB V	Sozialgesetzbuch – Fünftes Buch –
SGB VIII	Sozialgesetzbuch – Achtes Buch –
SGB X	Sozialgesetzbuch – Zehntes Buch –
SGG	Sozialgerichtsgesetz
SigG	Signaturgesetz
SIS	Schengener Informations-System
sog.	sogenannt
StGB	Strafgesetzbuch
StIdV	Steueridentifikationsnummerverordnung
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
StVZO	Straßen-Verkehrs-Zulassungs-Ordnung
SWIFT	Society for Worldwide Interbank Financial Telekommunications
Tb.	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
Tz.	Textziffer
u.a.	unter anderem
UIG	Umweltinformationsgesetz
UstG	Umsatzsteuergesetz
u.U.	unter Umständen
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VGV	Verbandsgemeindeverwaltung
VV	Verwaltungsvorschrift
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WM	Weltmeisterschaft
z.B.	zum Beispiel
ZBV	Zentrale Besoldungs- und Versorgungsstelle
Ziff.	Ziffer
ZPO	Zivilprozessordnung
z.T.	zum Teil

III. Glossar technischer Begriffe

ActiveX	Eine Softwaretechnologie von Microsoft. ActiveX erlaubt es, sogenannte Applets zu erstellen, die vom *Server* auf den Rechner des Internetnutzers übertragen und dort ausgeführt werden. Die Applets können dabei grundsätzlich auf alle Ressourcen des Zielrechners zugreifen, d.h. gegebenenfalls Daten lesen, löschen oder verändern.
Algorithmus	Beschreibung einer Verfahrensweise zur Lösung eines (mathematischen) Problems. Im Zusammenhang mit der *kryptografischen Verschlüsselung* steht der Begriff für die Art und Weise in der ein Klartext in ein *Chiffrat* umgewandelt wird und umgekehrt. Bekannte Algorithmen sind *DES*, *RSA*, oder *IDEA*.
Anonymisierung	Die Veränderung personenbezogener Daten in der Weise, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitszeit einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
ASP	Application Service Providing. Bereitstellung von Hard- und Softwarekomponenten an zentraler Stelle für eine Vielzahl von Anwendern. Meist mit dem Ziel verbunden, neben der Hard- und Software auch Dienstleistungen im Rahmen von Auftragsverhältnissen anzubieten (siehe auch *Hosting*).
Asymmetrische Verschlüsselung	Kryptografisches Verfahren, bei der zwei Schlüssel, ein öffentlicher und ein *geheimer Schlüssel*, verwendet werden. Der öffentliche Schlüssel ist jedem zugänglich, der geheime nur dem jeweiligen Empfänger einer Nachricht. Die Verschlüsselung folgt dabei folgendem Konzept: Wird mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselt, kann die Nachricht nur mit dem geheimen Schlüssel des Empfängers entschlüsselt werden. Mit umgekehrter Verwendung der Schlüssel lässt sich die digitale Signatur realisieren. Wird dabei mit dem geheimen Schlüssel des Absenders signiert, kann die Signatur anhand des öffentlichen Schlüssel des Absenders überprüft werden. Beispiele für asymmetrische Verfahren sind RSA und DSS.
ATM	Asynchronous Transfer Mode. Ein Kommunikationsprotokoll aus dem Bereich der Netzwerktechnik, d.h. eine Festlegung, in welcher Weise Daten über eine physikalische Leitung übertragen werden.
Attachment	Anhang zu einer *E-Mail*. Ein Attachment kann aus jeglicher Art von Daten bestehen, z.B. Dokumenten, Programmen, Bildern, Grafiken, Video- oder Audiodaten.
Authentisierung	Formeller Nachweis der Berechtigung zur Benutzung eines IT-Systems oder von dessen Ressourcen. Die Authentisierung erfolgt in Verbindung mit der *Identifikation* zumeist im Rahmen der Anmeldung an einem IT-System. Die Eingabe eines gültigen Passwortes ist ein Beispiel für eine Authentisierung.
Authentizität	Verlässliche Zurechenbarkeit einer elektronischen Nachricht zu einem bestimmten Absender.
Backbone	Bezeichnung für den Hauptstrang eines Netzwerks, über den der gesamte Datenverkehr zwischen den zentralen *Knotenrechnern* eines Netzes abgewickelt wird. Der Backbone stellt im Allgemeinen die höchsten Übertragungsraten innerhalb eines Netzes zur Verfügung.
Bandbreite	Maß für die Informationsmenge, die auf einem Kommunikationsanschluss innerhalb einer Zeiteinheit übertragen werden kann. Sie wird gemessen in Bit/Sekunde.

Browser	Programm auf dem Rechner des Benutzers zur Darstellung von Webseiten, d.h. von Inhalten im Internet. Gängige Browser sind der Microsoft Internet Explorer, der Netscape Navigator und der Mozilla Firefox.
Cache	Zwischenspeicher für die Speicherung von Kopien der Inhalte anderer Speichermedien, insbesonderer für Daten, auf die häufiger zugegriffen wird. Er beschleunigt damit den Zugriff. Bei Internet-Suchmaschinen halten Cache-Speicher die Daten vor, die beim letzten Suchdurchgang erfasst wurden. Falls zwischen zwei Suchläufen Änderungen an einer Interseite erfolgt sind, enthält der Cache in der Regel noch den vorherigen Stand.
Callback	Automatischer Rückruf. Verfahren bei *Wählleitungsverbindungen*, bei welchem ein angewählter Rechner den Verbindungswunsch registriert, die Verbindung abbricht und in umgekehrter Richtung erneut aufbaut. In Verbindung mit Rufnummernlisten kann damit erreicht werden, dass eine Verbindung nur zu einem bestimmten Anschluss hergestellt wird.
CERT-Advisories	Sicherheitshinweise der Computer Emergency Response Teams, einer Sicherheitsorganisation für das Internet. Ein deutschsprachiges CERT existiert für das Deutsche Forschungsnetz (DFN) unter der Internetadresse http://www.cert.dfn.de/
CHAP	Challenge Authentication Protocol. Automatisches Verfahren zur *Authentisierung* bei welchem dem rufenden Anschluss eine binäre Zufallszahl (challenge) zur Verfügung gestellt wird. Diese wird mit einem vorgegebenen *Algorithmus* verarbeitet und das Ergebnis dem gerufenen Anschluss übermittelt. Entspricht das Zurückgelieferte dem erwarteten Ergebnis, wird die Verbindung hergestellt.
Chat	Eigentlich IRC – Internet Relay Chat. Bezeichnung eines Internetdienstes, der die Möglichkeit bietet online zu diskutieren. Die Beiträge werden über die Tastatur eingegeben. Thematisch orientierte Chat-Foren eröffnen die Möglichkeit der Online-Diskussionen mit mehreren Teilnehmern gleichzeitig.
Chiffrat	Ergebnis einer *kryptografischen Verschlüsselung*, d.h. die mittels *Algorithmus* und Schlüssel verschlüsselten Daten.
Client	Begriff aus dem Netzwerkbereich: Ein Client nimmt von einem *Server* angebotene Dienste in Anspruch. Der Client schickt Anfragen an den Server und stellt dessen Antworten in lesbarer Weise auf dem Bildschirm dar. Als Clients werden sowohl Rechner, z.B. PC, als auch Prozesse, z.B. Programmfunktionen, bezeichnet.
Client-/Server-Architektur	Modell einer Netzwerkstruktur oder eines Softwarekonzepts, bei der / bei dem eine hierarchische Aufgabenverteilung vorliegt. Der Server ist dabei der Anbieter von Ressourcen, Funktionen oder Daten – die Arbeitsstationen (Clients) nehmen diese in Anspruch.
CLIP	Calling Line Identification Protocol. Anzeige der Nummer des rufenden Anschlusses beim gerufenen Teilnehmer. Die über CLIP bereitgestellte Anschlussnummer kann für die Prüfung der Zugangsberechtigung genutzt werden.
CUG	Closed User Group (Geschlossene Benutzergruppe). Leistungsmerkmal von Kommunikationsdiensten, bei welchem die zugelassenen Anschlüsse in einer Berechtigungstabelle eingetragen werden. Kommunikationsanforderungen von in dieser Tabelle nicht enthaltenen Anschlüssen werden zurückgewiesen.
Denial-of-Service-Attacke	Angriff, bei welchem durch die Ausnutzung von Schwachstellen in Programmen, Protokollen oder Konfigurationen die Funktionsfähigkeit von Rechnern oder Serverdiensten beeinträchtigt wird. Eine Denial-of-Service-Attacke kann jedoch auch in der vorsätzlichen Überlastung von Diensten bestehen (vgl. *Spam-Mail*).

DES	Data Encryption Standard. Von IBM in den 70er Jahren entwickeltes symmetrisches Verschlüsselungsverfahren. Bei DES werden Datenblöcke zu je 64 Bits mit einem 56-Bit-Schlüssel codiert. DES ist weit verbreitet und wurde mit der Standardschlüssellänge bereits kompromittiert, d.h. innerhalb überschaubarer Zeit entschlüsselt. Höhere Sicherheit bietet Triple DES (DES 3) bei welchem mehrere Verschlüsselungsrunden aufeinander folgen.
DICOM	Im Bereich der Medizin genutztes Kommunikationsprotokoll für die Übertragung von Radiologiedaten.
Dienst	Sammlung von Ressourcen (Funktionen, Daten), die von einem *Server* gegenüber den zugehörigen *Clients* angeboten werden. Typische Dienste sind E-Mail, Filetransfer, Einwahl oder WWW.
Directory-Traversal	Vorgehensweise, bei der in missbräuchlicher Absicht versucht wird, die für ein Internet-Angebot oder Webanwendung vorgegebenen Zugriffspfade zu verlassen.
DFÜ	Datenfernübertragung
Dial-in	Auch Einwahl oder *Inbound* genannt. Vorgang bei dem ein entfernter Anschluss eine Kommunikationsverbindung zum lokalen IT-System herstellt.
Dial-out	Auch *Outbound* genannt. Vorgang bei dem eine Kommunikationsverbindung zu einem entfernten IT-System hergestellt wird.
D-Kanal-Filter	Programm zur Überwachung der Kommunikation auf dem Steuerungskanal des *ISDN*-Dienstes.
DNS	Domain Name Service. Internetdienst der *IP-Adressen* in leichter zu merkende Rechnernamen umsetzt (z.B. 192.168.100.10 in www.firma.de)
DNS-Server	Rechner bzw. Programme, welche DNS-Dienste bereitstellen.
Domain Name Service	siehe *DNS*
Download	Herunterladen von Daten aus dem Internet auf das eigene IT-System.
DSS	Digital Signature Standard. Ein Kryptografisches Verfahren für die d*igitale Signatur.*
Einwahlknoten	Technische Komponente, die den Zugang zu einem Kommunikationsnetz über eine Wählleitung (z.B. über Telefon) ermöglicht.
Elektronische Signatur	„Elektronische Unterschrift“. Verfahren bei welchem durch die Verwendung *asymmetrischer Verschlüsselungsverfahren,* meist in Kombination mit *Hashverfahren* die *Authentizität* und, je nach Art der Signatur, *die Integrität* einer elektronischen Nachricht sichergestellt werden kann. Eine gesetzliche Sicherheitsvermutung besteht für Signaturverfahren nach dem Signaturgesetz.
E-Mail	Electronic Mail (Elektronische Post). E-Mail ermöglicht das Verschicken elektronischer Nachrichten. Diesen können Dokumente, Programme, Bilder, Grafiken, Video- oder Audiodaten in Form von *Attachments* beigefügt werden.
Ende-zu-Ende-Verschlüsselung	Verschlüsselung des Datenverkehrs zwischen den Kommunikationsteilnehmern. Die Ende-zu-Ende-Verschlüsselung erfolgt im Gegensatz zur *Leitungsverschlüsselung* auf der Anwendungsebene, d.h. bei der Nutzung von Programmen. So muss z.B. eine E-Mail-Nachricht als solche explizit verschlüsselt werden.

Faxserver	Rechner oder Programme welche Faxdienste (Versand, Empfang) bereitstellen.
Firewall	„Brandmauer“. Ein System in Form von Hard- und/oder Software, das den Datenfluss zwischen einem internen und einem externen Netzwerk kontrolliert bzw. ein internes Netz vor Angriffen von außerhalb, z.B. aus dem Internet, schützt.
Fortgeschrittene elektronische Signatur	Signaturlösung nach § 2 Nr. 2 Signaturgesetz (SigG). Sie ermöglicht im Vergleich zur einfachen *elektronischen Signatur* nach § 2 Nr. 1 SigG die Identifizierung des Signaturschlüsselinhabers und ist mit den signierten Daten, so verknüpft, dass eine nachträgliche Veränderung erkannt werden kann.
Freie Abfragesprache	Programmiersprache mit der beliebige Abfragen an Datenbanksysteme gerichtet werden können. Eine bekannte freie Abfragesprache ist die Structured Query Language.
FTP	File Transfer Protokoll. Speziell auf die Übertragung von Datenbeständen ausgerichtetes Kommunikationsprotokoll aus der Familie der Internetprotokolle.
Gateway	Ein Gateway ist ein Rechner am Übergang zwischen zwei Netzen der die notwendige Umsetzung bei Verwendung unterschiedlicher *Protokolle* sicherstellt, bzw. den Empfang und die Weiterleitung von Daten steuert.
Geheimer Schlüssel	siehe *Private Key.*
Geräte-ID	Eindeutige Kennzeichnung bestimmter Hardware(komponenten).
Geschlossene Benutzergruppe	siehe *CUG.*
GnuPP	GnuPP, GNU Privacy Projekt, ist eine vom Bundeswirtschaftsministerium geförderte Software zur E-Mail-Verschlüsselung. GnuPP ist kompatibel zu der verbreitet eingesetzten Lösung Pretty Good Privacy *PGP.* Anders als bei dieser handelt es sich bei GnuPP um *Open Source Software.*
Handheld-PC	Computer in Taschenbuchgröße und kleiner, meist ohne integrierte Tastatur, jedoch mit Sensorbildschirm. Bedienbar mit einem geeigneten Stift.
Hashverfahren	Mathematisches Verfahren mit dem ein (langes) elektronisches Dokument auf eine (kurze) Prüfsumme abgebildet wird. Änderungen am Dokument, auch geringste, führen bei erneutem „hashen“ zu einer anderen Prüfsumme. Hashverfahren werden im Rahmen der d*igitalen Signatur* für den Nachweis der Integrität einer Nachricht benötigt.
Hashwert	Prüfsumme als Ergebnis eines Hashvorgangs.
Homepage	Start- und Begrüßungsseite eines Internetangebotes. Von der Homepage gelangt man über Verweise (links) zu den weiteren Inhalten des Angebots.
Hosting	Technische Dienstleistung, in deren Rahmen der Betrieb von Systemen und / oder Anwendungen in geeigneten Räumlichkeiten des Auftragnehmers erfolgt.
HTML	Hypertext Markup Language. Eine Programmiersprache, in der *Webseiten* geschrieben werden. Der *Browser* ermöglicht die grafische Umsetzung der HTML-Befehle. Das besondere an HTML sind die Einsetzbarkeit auf verschiedenen Systemen (Windows, Unix, Macintosh usw.) und die Verweise (Hyperlinks) auf andere *Webseiten* auf dem lokalen System oder im Internet.
HTTP	Hypertext Transfer Protocol. Internetprotokoll zur Darstellung vom *HTML*-Seiten via *Browser.*

Hyperlink	siehe *HTML*. Verweis auf andere Webseiten auf dem lokalen System/Netzwerk oder andere Rechner im Internet.
IDEA	International Data Encryption Algorithm. *Ein symmetrisches Verschlüsselungsverfahren* mit einer Schlüssellänge von 64 bzw. 128 Bit.
Identifikation	Nachweis über die Identität eines Benutzers eines IT-Systems, z.B. anhand einer Benutzerkennung (User-ID). Die Identifikation erfolgt in Verbindung mit der *Authentisierung* zumeist im Rahmen der Anmeldung an einem IT-System.
IMSI	„International Mobile Subscriber Identity“ (Internationale Kennungen für mobile Teilnehmer) Die IMSI dienen der international eindeutigen Identifikation von Teilnehmern in drahtlosen und drahtgebundenen Kommunikationsdiensten. Bei Mobiltelefonen ist die IMSI auf der SIM-Karte gespeichert. (siehe auch *SIM-Karte*)
Inbound	siehe *Dial-in*.
Integrität	In der Informationstechnik die Vollständigkeit und Unversehrtheit elektronisch gespeicherter Daten.
Internetadresse	Angabe unter welcher Bezeichnung Informationen oder Dienste im Internet angesprochen werden können. Die Internetadresse wird meist als URL (Uniform Ressource Locator) angegeben. Eine typische Internetadresse ist z.B.: http://www.datenschutz.rlp.de/
Intranet	Internes Computernetzwerk, das technisch auf den im Internet verwendeten Protokollen basiert.
IP-Adresse	Internet Protocol Adresse. Numerische Angabe für die eindeutige Bezeichnung eines Rechners im Internet (z.B. 192.168.100.10); siehe auch *TCP/IP*.
IP-Protokoll	Kommunikationsprotokoll im Internet. Die Datenübertragung erfolgt dabei in einzelnen Paketen, deren Absender und Empfänger durch *IP-Adressen* gekennzeichnet werden.
IPSec-Protokoll	Erweiterung des IP-Protokolls um Funktionen zur Sicherung der Vertraulichkeit und Integrität der Kommunikation.
ISDN	Integrated Services Digital Network. Kommunikationsprotokoll über das verschiedene Kommunikationsdienste wie Telefonie, Telefax, Datenkommunikation, Bildtelefon usw. in digitaler Form erbracht werden können.
ISDN-Dienstekennung	Bezeichnung des jeweiligen Kommunikationsdienstes innerhalb des ISDN-Protokolls.
ISDN-Leistungsmerkmal	Einzelne Funktion innerhalb eines ISDN-Dienstes. Beispielsweise die Übermittlung der Rufnummer an den Gesprächspartner beim ISDN-Telefondienst.
ISDN-Router	*Router* der das ISDN-Protokoll unterstützt.
Javascript	Eine von den Firmen SUN und Netscape entwickelte Makrosprache. Die damit erstellten Anweisungen (scripts) werden vom Browser des Clientrechners interpretiert und ausgeführt (siehe auch *ActiveX*).
Knotenrechner	Vermittlungskomponente innerhalb eines Netzwerks (z.B. Router), die die Datenübertragung steuert.

Kompilierung	Vorgang zur Umwandlung des Quellcodes eines Programms in *Maschinencode*, den Befehlssatz des jeweiligen Prozessors.
Kryptobox	Komponente, die entsprechend voreingestellter Parameter für eine Kommunikationsverbindung eine kryptografische Absicherung gewährleistet. Sie erfordert empfängerseitig eine entsprechende Gegenstelle. Kryptoboxen machen benutzerseitige Eingriffe für eine Verschlüsselung oder Integritätssicherung i.d.R. entbehrlich.
Kryptografische Verschlüsselung	Verfahren bei welchem mit Hilfe eines kryptografischen *Algorithmus* Klartexte in ein *Chiffrat* umgewandelt, d.h. verschlüsselt werden. Die Wiederherstellung des ursprünglichen Klartextes ist nur mit Kenntnis des jeweiligen Schlüssels möglich.
LAN	Local Area Network. Internes Computernetz einer Verwaltung, Einrichtung u.ä.
LDKN	Das vom Daten- und Informationszentrum betriebene Landesdaten- und Kommunikationsnetz Rheinland-Pfalz (siehe auch *rlp-Netz*)
Leitungsverschlüsselung	Verschlüsselung des Datenverkehrs auf der physikalischen Ebene zwischen den Anschlusskomponenten einer Kommunikationsverbindung (Leitung oder Funkstrecke). Die Leitungsverschlüsselung erfolgt im Gegensatz zur *Ende-zu-Ende-Verschlüsselung* unabhängig von der jeweiligen Anwendung (z.B. E-Mail). Sie wird i.d.R. über technische Komponenten (Verschlüsselungsboxen, Router) realisiert und erfasst alle Datenübertragungen auf der betroffenen Kommunikationsverbindung. Ein Zutun des Benutzers ist anders als bei der Ende-zu-Ende-Verschlüsselung nicht erforderlich.
Mailgateway	Vermittlungsrechner, der die Entgegennahme und Weiterleitung von E-Mail-Nachrichten steuert.
Mailserver	IT-System bzw. Anwendung, über die Elektronische Post (E-Mail) entgegengenommen und verschickt werden kann.
Maschinencode	Die im Rahmen der *Kompilierung* aus dem Quellcode erzeugten und an den Befehlssatz des jeweiligen Prozessors angepassten binären Programmbefehle.
Message Authentication Code	Angabe anhand derer die *Authentizität* einer Nachricht überprüft werden kann.
Network Information Center (NIC)	Kontrollzentrum eines Netzwerkes in welchem die Administration und Überwachung des Netzes konzentriert sind.
OCR	Optical Character Recognition. Verfahrens zur automatisierte Erkennung und Erfassung von Texten.
Öffentlicher Schlüssel	siehe *Public Key.*
Open Source Software	Software, deren *Quellcode* (Source) offen gelegt wurde und durch jedermann grundsätzlich frei vervielfältigt, verändert und verbreitet werden darf. Die bekannteste lizenzrechtliche Grundlage von Open Source Software ist die GNU Public License (GPL).
Oracle	Produktbezeichnung eines Datenbankverwaltungsprogramms.
Oracle-Instanz	Bezeichnung für eine Datenbank, die innerhalb der Oracle-Software eine abgeschottete Einheit bildet.
Outbound	siehe *Dial-out.*
Overlay-Netz	Ein Netz aus Netzen, d.h. ein Netzwerk dessen Knoten wiederum aus Netzwerken bestehen.

PAP	Password Authentication Protocol. Kommunikationsprotokoll bei dem die *Authentisierung* über Passworte erfolgt.
Penetrationstest	Der gezielte Test der Möglichkeiten, von außen mit den einem Angreifer verfügbaren Mitteln in ein geschütztes Netz einzudringen.
PGP	Pretty Good Privacy. Ein weitverbreitetes Programm zur Verschlüsselung und digitalen Signatur auf der Basis *asymmetrischer Verschlüsselungsverfahren*. Das Verfahren gilt bei Verwendung ausreichender Schlüssellängen (> 1.024 Bit) derzeit als sicher.
PKI	Public Key Infrastructure. Gesamtheit der für die Verwendung von *Public Key* Verfahren erforderlichen Komponenten und Dienste (u.a. Schlüsselerzeugung, Zertifizierungs-, Verzeichnis-, Sperr- und Zeitstempeldienste).
Pretty Good Privacy	siehe *PGP*.
Private Key	Geheimer Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens* der nur dem Empfänger einer verschlüsselten Nachricht bzw. dem digital Signierenden bekannt sein darf. Der geheime Schlüssel dient der Entschlüsselung einer mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselten Nachricht. Eine mit einem geheimen Schlüssel erzeugte Signatur kann nur mit dem öffentlichen Schlüssel des Erzeugers der Signatur verifiziert werden.
Protokoll	Technische Regelung über den Aufbau und die Größe von Datenpaketen und die Art und Weise, wie diese im Rahmen einer Kommunikation übertragen werden.
Pseudonymisierung	Das Ersetzen des Namens oder anderer Identifikationsmerkmale einer natürlichen Person durch ein Kennzeichen zu dem Zweck, die Bestimmung der Betroffenen auszuschließen oder wesentlich zu erschweren. Im Gegensatz zur Anonymisierung ist mit Kenntnis der Zuordnungsregel meist ohne größeren Aufwand umkehrbar.
Public Key	Öffentlicher Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens* der allen Teilnehmern bekannt sein muss. Zum Verschlüsseln wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die Entschlüsselung erfolgt durch den Empfänger mit dessen *geheimen Schlüssel*. Bei der digitalen Signatur wird durch den Absender mit dessen geheimen Schlüssel signiert, und die Signatur beim Empfänger mit dem öffentlichen Schlüssel des Absenders verifiziert.
Qualifizierte elektronische Signatur	Elektronische Signatur nach § 2 Nr. 3 Signaturgesetz (SigG) Sie beruht im Gegensatz zur *fortgeschrittenen elektronischen Signatur* auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat nach SigG und genügt bei ihrer Erzeugung höheren technischen Anforderungen. Sie ist, sofern gesetzlich zugelassen, die Alternative zur eigenhändigen Unterschrift.
Quellcode	Der in einer Programmiersprache vorliegende, noch nicht in Maschinencode umgewandelte Programmcode (vgl. *Kompilierung*). Quellcodeanweisungen ermöglichen aufgrund der im Vergleich zum *Maschinencode* höheren Abstraktionsebene grundsätzlich eine Analyse der jeweiligen Programmbefehle.
Query-ID	Bei der Anfrage an einen *DNS-Server* vergebene Bezeichnung zur Unterscheidung der verschiedenen DNS-Anfragen (queries).
Relationales Datenbanksystem	Datenbanksystem, bei welchem Daten nicht in fest vorgegebenen Strukturen sondern in Tabellen vorgehalten werden, die über frei definierbare Relationen untereinander verknüpft werden können.

Replay Attack	Angriff, bei welchem ein Datenstrom (z.B. die Passworteingabe an einem IT-System) aufgezeichnet und zu einem späteren Zeitpunkt erneut eingespielt wird. Der Angriff funktioniert bei Kenntnis der Struktur des Datenstroms auch dann, wenn dieser verschlüsselt ist.
RFID	Radio Frequency Identification. Infomationsträger, die berührungslos per Funk ausgelesen werden können.
rlp-Netz	siehe *LDKN*
Router	Technische Komponente, die die Wegefindung (routing) und Übermittlung in einem Netzwerk steuert. Mit routing bezeichnet man den Weg der Datenpakete innerhalb von Netzen. Das Internet kennt keine Direktverbindungen zwischen Rechnern. Statt dessen erfolgt der Versand von Daten in kleinen Paketen und nach Bedarf über verschiedene Zwischensysteme auf dem zum Übermittlungszeitpunkt günstigsten Weg. Diese Form des Datenverkehrs ermöglicht die hohe Flexibilität und Ausfallsicherheit des Internet.
RSA	Aus den Anfangsbuchstaben der Erfinder (Rivest, Shamir und Adleman) zusammengesetzte Bezeichnung für ein *asymmetrisches Verschlüsselungsverfahren.*
Schlüssellänge	Angabe über die Länge kryptografischer Schlüssel in Bit. Grundsätzlich gilt: je länger ein Schlüssel, desto größer ist die Zahl der möglichen Ausprägungen und desto höher der Aufwand zu seiner Kompromittierung.
Schlüsselpaar	Das Paar aus geheimem und öffentlichem Schlüssel bei *asymmetrischen Verschlüsselungsverfahren.*
Server	Zentraler Rechner in einem Netzwerk, der den Arbeitsstationen/Clients Daten, Dienste usw. zur Verfügung stellt. Auf dem Server ist das Netzwerkbetriebssystem installiert, und vom Server wird das Netzwerk verwaltet. Als Server werden neben Rechnern auch Softwarekomponenten bezeichnet, die *Client*-Prozessen, z.B. Internet-browsern, Informationen und Funktionen zur Verfügung stellen.
Session-Key	Kryptografischer Schlüssel, der nur für eine bestimmte Zeit (session) verwendet wird und danach seine Gültigkeit verliert.
SIM-Karte	„Subscriber Identity Module“ Chipkarte, die ein Kennzeichen zur eindeutigen Identifizierung des Teilnehmers des Kommunikationsdienstes ermöglicht. (siehe auch *IMSI*)
SMTP	Simple Mail Transfer Protocol. Kommunikationsprotokoll für die elektronische Post im Internet (siehe *E-Mail*).
Spam-Mail	Die Überflutung von (elektronischen) Postfächern mit unerwünschter *E-Mail* mit dem Ziel, die Funktionsfähigkeit des Mailservers zu beeinträchtigen (siehe *Denial-of-Service-Attacke*).
Spoofing	Vorgehensweise bei der sich jemand als ein anderer Benutzer, Absender oder Rechner ausgibt, um unbefugten Zugriff auf Daten oder IT-Systeme zu erhalten.
SQL	Structured Query Language ist eine Datenbanksprache zur Beschreibung, Veränderung und Abfrage von Daten in relationalen Datenbanken. SQL ist standardisiert und wird von fast allen gängigen Datenbanksystemen unterstützt.
SSL	Secure Socket Layer. Ein Sicherheitsprotokoll, das *Client-/Server*-Anwendungen eine Kommunikation ermöglicht, die nicht abgehört oder manipuliert werden kann.

Standleitung	Kommunikationsverbindung die im Gegensatz zu einer *Wählleitungsverbindung* permanent und in der Regel exklusiv für bestimmte Teilnehmer geschaltet ist.
Subnetz	Teil eines Kommunikationsnetzes, der von anderen Teilen des Netzes abgegrenzt ist. Die Subnetzbildung kann logisch erfolgen, z.B. durch die Verwendung entsprechender Netzadressen oder physikalisch durch den Einsatz einer die Kommunikation steuernde Netzkomponente am Übergang des Subnetzes zum restlichen Netz.
Symmetrische Verschlüsselung	Verschlüsselungsverfahren, bei welchem im Gegensatz zu *asymmetrischen Verfahren* für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser muss damit dem Empfänger einer Nachricht auf einem zweiten sicheren Kanal zugeleitet werden.
TESTA-Netz	Trans European Services für Telematics between Administrations. Netzplattform für die Kommunikation öffentlicher Verwaltungen.
TCP/IP	Transmission Control Protocol/Internet Protocol. Standardkommunikations-*Protokoll* im Internet. Das Internet Protocol (IP) dient der Fragmentierung und Adressierung von Daten und übermittelt diese vom Sender zum Empfänger. Das Transmission Control Protocol (TCP) baut darauf auf, sorgt für die Einsortierung der Pakete in der richtigen Reihenfolge beim Empfänger und bietet die Sicherstellung der Kommunikation durch Bestätigung des Paketempfangs. Es korrigiert Übertragungsfehler automatisch.
TCP-Sequence Number	Aufsteigende Nummer, die die logische Reihenfolge der Datenpakete einer Datenübertragung festlegt. Die im Internet auf ggf. unterschiedlichen Wegen übertragenen Pakete werden anhand der TCP-Sequence Number beim Empfänger wieder zusammengesetzt.
Tunneling	Verfahren zur Absicherung einer Datenübertragung über unsichere oder nicht vertrauenswürdige Kommunikationsverbindungen mit Hilfe kryptografischer Verfahren.
Transaktionsnummer	Eindeutige, einmalig verwendbare Angabe, die die *Authentizität* einer Transaktion belegt. Transaktionsnummern werden in der Regel im Voraus erzeugt. Sie sind eindeutig, einem bestimmten Absender zugeordnet und müssen bis zu ihrer Verwendung geheim gehalten werden. Der Empfänger prüft die Verbindung Absenderangabe/Transaktionsnummer und erhält im Fall der Gültigkeit so einen Nachweis über den Urheber einer Transaktion. Nach ihrer Verwendung verfällt die Transaktionsnummer.
Triple DES	Verfahren, bei welchem der Verschlüsselungsalgorithmus *DES* in drei aufeinanderfolgenden Durchgängen durchlaufen wird. Triple DES bietet eine höhere Sicherheit gegenüber Entschlüsselungsversuchen als der einfache *DES*.
Trojanisches Pferd	Programm mit Schadensfunktionen, die zeit- oder ereignisgesteuert ohne Wissen des Benutzers im Hintergrund aktiv werden. Häufig wird dem Benutzer vordergründig eine nützliche oder sinnvolle andere Funktion vorgegaukelt.
Trustcenter	Stelle, die im Rahmen des Einsatzes von Verschlüsselungsverfahren zentrale Funktionen wahrnimmt. Beispiele hierfür sind die Erzeugung kryptografischer Schlüssel, die Erteilung und Verwaltung von *Zertifikaten* sowie der Betrieb von *Verzeichnisdiensten*.
URL	Uniform Resource Locator. Angabe zur Fundstelle einer Ressource in Computernetzwerken und des Protokolls für den Zugriff auf diese.
UserID	Benutzerkennung

Verzeichnisdienst	*Server*dienst in welchem Personen und Ressourcen mitsamt zugehörigen Attributen katalogisiert werden. Verzeichnisdienste werden z.B. als Adressverzeichnisse für die elektronische Post oder im Rahmen des Einsatzes von Signatur und Verschlüsselungsverfahren für die Verwaltung von *Zertifikaten* eingesetzt.
Virtuelles Privates Netz	Logisches Netz auf physikalischen Kommunikationsverbindungen. Die *VPN*-Technologie ermöglicht es, verschiedene, die gleiche Infrastruktur nutzenden Netze gegeneinander abzuschotten.
Voice-over-IP	siehe *VoIP*
VoIP	„Voice-over-IP“ Eine Technologie auf Basis des Internetprotokolls, die es erlaubt, Telefoniedienste in paketvermittelnden Datennetzen zu übertragen.
VPN	*Virtuelles Privates Netz.*
Wählleitungsverbindung	Kommunikationsverbindung die im Gegensatz zu einer *Standleitung* nur bei Bedarf durch Anwahl des gewünschten Anschlusses aufgebaut wird.
Webanwendung	Programm bzw. Verfahren, das auf einem Webserver bereitgestellt wird und, zumeist via Internet, über einen Browser aufgerufen und bedient werden kann.
Webseite	Seite eines Angebots im *World Wide Web.*
Webserver	IT-System bzw. Anwendung die im Internet oder Intranet Inhalte bereitstellt, auf die mit den gängigen Internetprotokollen zugegriffen werden kann.
Word Wide Web	Weltweites Netz. Auch als WWW oder W3 bezeichnet. Gemeint ist ein Dienst im Internet, der sich durch hohe Benutzerfreundlichkeit auszeichnet und zur Verbreitung des Internets massiv beigetragen hat. Entwickelt wurde das World Wide Web von Wissenschaftlern, die auf einfache Art Informationen austauschen wollten. Der Zugriff auf die Informationen erfolgt über WWW-*Browser.*
WWW	siehe *Word Wide Web.*
X.500	Protokoll für den Betrieb und die Kommunikation mit *Verzeichnisdiensten.*
Zertifikat	Im Rahmen digitaler Signaturverfahren die Beglaubigung über die Gültigkeit eines öffentlichen Schlüssels und dessen Zuordnung zu einer bestimmten Person oder Stelle.

IV. Bisherige Tätigkeitsberichte des Ausschusses für Datenschutz, der Datenschutzkommission und des Landesbeauftragten für den Datenschutz Rheinland-Pfalz

1. Tätigkeitsbericht	Drucksache 7/3342	vom 17. Oktober 1974
2. Tätigkeitsbericht	Drucksache 8/350	vom 1. Oktober 1975
3. Tätigkeitsbericht	Drucksache 8/1444	vom 1. Oktober 1976
4. Tätigkeitsbericht	Drucksache 8/2470	vom 10. Oktober 1977
5. Tätigkeitsbericht	Drucksache 8/3492	vom 12. Oktober 1978
6. Tätigkeitsbericht	Drucksache 9/253	vom 15. Oktober 1979
7. Tätigkeitsbericht	Drucksache 9/970	vom 15. Oktober 1980
8. Tätigkeitsbericht	Drucksache 9/1869	vom 28. Oktober 1981
9. Tätigkeitsbericht	Drucksache 10/270	vom 26. Oktober 1983
10. Tätigkeitsbericht	Drucksache 10/1922	vom 8. November 1985
11. Tätigkeitsbericht	Drucksache 11/710	vom 11. November 1987
12. Tätigkeitsbericht	Drucksache 11/3427	vom 21. Dezember 1989
13. Tätigkeitsbericht	Drucksache 12/800	vom 16. Dezember 1991
14. Tätigkeitsbericht	Drucksache 12/3858	vom 12. November 1993
15. Tätigkeitsbericht	Drucksache 12/7589	vom 16. November 1995
16. Tätigkeitsbericht	Drucksache 13/2427	vom 15. Dezember 1997
17. Tätigkeitsbericht	Drucksache 13/4836	vom 18. Oktober 1999
18. Tätigkeitsbericht	Drucksache 14/486	vom 22. November 2001
19. Tätigkeitsbericht	Drucksache 14/2627	vom 5. November 2003
20. Tätigkeitsbericht	Drucksache 14/4660	vom 14. November 2005

1. Vorbemerkungen

Nach 16 Jahren endete im April die Amtszeit von Prof. Dr. Walter Rudolf, dem ersten Landesbeauftragten für den Datenschutz in Rheinland-Pfalz. Acht Tätigkeitsberichte sind unter seiner Verantwortung entstanden. Auch dieser 21. Bericht fasst – mit Ausnahme der Monate April bis September 2007 – noch datenschutzrechtlich relevante Vorgänge aus seiner Amtszeit zusammen. Auf über 1.300 Seiten sind so die datenschutzrechtlichen Probleme und Entwicklungen von mehr als eineinhalb Jahrzehnten dokumentiert, außerdem sein stetiges und insgesamt auch erfolgreiches Bemühen – gemeinsam mit den Verantwortlichen in Parlament, Regierung und Verwaltung – dem Datenschutz im Lande Geltung zu verschaffen. Dafür ist Prof. Rudolf über die Jahre hinweg und vor allem auch anlässlich seines Ausscheidens aus dem Amt des LfD vielfach gedankt worden.

Dieser Dank soll zu Beginn dieses Tätigkeitsberichts noch einmal wiederholt und mit der Feststellung verbunden werden, dass die Maximen, die in den zurückliegenden 16 Jahren die Amtausübung des LfD geprägt haben, auch in Zukunft maßgeblich bleiben werden. Dazu gehört vor allem der Anspruch, den Datenschutz mit Augenmaß zu betreiben. Ein solches Amtsverständnis empfiehlt sich nicht nur deshalb, weil es in der Vergangenheit erfolgreich praktiziert wurde, sondern weil es von der Einsicht getragen wird, dass in einer offenen Gesellschaft und in einer parlamentarischen Demokratie der Schutz der Privatsphäre mit anderen Grundrechten und Grundprinzipien in einen vernünftigen und verträglichen Ausgleich gebracht werden muss, wobei sicherlich auch zu akzeptieren ist, dass das, was gestern noch zur Privatsphäre gezählt wurde, heute oder morgen schon dem Bereich des Öffentlichen angehört.

Mit anderen Worten: Es gibt nicht nur den Datenschutz und auch die Privatsphäre ist nicht das Maß aller Dinge. Aber der Datenschutz darf auch nicht vernachlässigt oder gar gering geschätzt werden. Er ist Teil der Menschenwürde und Teil unserer demokratischen Grundordnung und damit von grundlegender Bedeutung. Staat und Gesellschaft sind fraglos auf einen funktionierenden Datenschutz und damit auf eine hinreichend geschützte Privatsphäre angewiesen.

Als Leitlinie für den LfD taugt der Datenschutz mit Augenmaß aber nur dann, wenn Parlament, Regierung und Verwaltung ihrerseits achtsam und respektvoll mit dem in der Landesverfassung verankerten informationellen Selbstbestimmungsrecht umgehen. In den zurückliegenden Jahrzehnten war dies in Rheinland-Pfalz der Fall. Das Land hat – nach Hessen – als zweites Bundesland ein Datenschutzgesetz erlassen, als eines der ersten alten Bundesländer den Datenschutz in der Landesverfassung verankert und ihm auch beim Erlass und dem Vollzug seiner Gesetze in aller Regel Rechnung getragen.

Bei dieser insgesamt datenschutzfreundlichen Grundeinstellung muss es aber auch in Zukunft bleiben. Die neuen technischen Möglichkeiten und die neuen Herausforderungen, insbesondere im Bereich der inneren Sicherheit, dürfen die staatlichen Organe nicht von diesem Weg abbringen. Das bedeutet vor allem, dass Landtag und Landesregierung nicht der Versuchung erliegen dürfen, beim Erlass datenschutzrelevanter Gesetze die Belastbarkeit der Verfassung bzw. die Grenzen des verfassungsrechtlich gerade noch Zulässigen auszutesten. Die Gefahr ist zu groß, dass dabei am Ende doch Grenzen überschritten werden. Das Bundesverfassungsgericht hat dies für Bundesgesetze in den letzten Jahren mehrfach feststellen müssen. Dies schadet nicht nur dem Datenschutz, sondern beschädigt auch das Vertrauen, das die Bürger*) in das Handeln ihrer Repräsentanten investieren und auf das diese dringend angewiesen sind. Der Landesgesetzgeber bleibt deshalb aufgerufen, aus Respekt vor der privaten Lebensgestaltung der Bürger dem Datenschutz Raum zu geben und ihn nicht auf einen Kernbereich zurückzudrängen.

Auch an einer anderen – nicht nur formalen – Übung aus der Amtszeit von Prof. Rudolf soll festgehalten werden. Der Tätigkeitsbericht wird auch in Zukunft nicht in der „Ich-Form“, sondern unter der Bezeichnung „Landesbeauftragter für den Datenschutz (LfD)“ abgefasst. Auf diese Weise soll die Verantwortung des LfD als oberste Landesbehörde zum Ausdruck gebracht werden. Zwei Ausnahmen möchte ich mir an dieser Stelle erlauben.

Die erste soll es mir ermöglichen, mich im Rahmen des Vorwortes bei den Lesern des Tätigkeitsberichtes vorzustellen: Der Landtag Rheinland-Pfalz hat mich im März 2007 auf Vorschlag aller im Landtag vertretenen Fraktionen bei nur wenigen Gegenstimmen und Enthaltungen mit großer Mehrheit gewählt. Einen Monat später habe ich dieses Amt angetreten. Davor war ich in verschiedenen Funktionen über 25 Jahre in der Verwaltung des Landtags tätig, u.a. als Leiter des Wissenschaftlichen Dienstes und ab 2001 als Leiter der Abteilung für Kommunikation und Information. Diese Zeit – der noch ein Jahr als Verwaltungsrichter vorangegangen war – hat mich geprägt und zu einem überzeugten und uneingeschränkten Anhänger unserer repräsentativen und parlamentarischen Demokratie gemacht.

*) Im Sinne einer besseren Lesbarkeit werden Begriffe wie Bürger, Betroffener, Beschwerdeführer etc. geschlechtsneutral verwendet, wenngleich immer beide Geschlechter gemeint sind.

Dies wird sich selbstverständlich auch in meinem Amtsverständnis als LfD niederschlagen. Landtag und Landesregierung sind – wie es in der Landesverfassung heißt – die „Organe des Volkswillens". **Sie** entscheiden über die wesentlichen politischen Angelegenheiten im Land, und **sie** tragen dafür auch die Verantwortung. Der LfD hat – bezogen auf den Bereich des Datenschutzes – nur eine dienende – besser gesagt: eine unterstützende – Funktion. Er hat seinen Teil dazu beizutragen, dass die Verantwortlichen in Parlament und Regierung ihre Verantwortung für den Datenschutz guten Gewissens tragen können. Er tut dies nach dem Landesdatenschutzgesetz durch Kontrolle und vor allem durch Beratung. Ich weiß, dass dieser Rat gerade in einer Zeit gravierender technischer Entwicklungen und der genannten neuen Gefahren auch erwartet – zum Teil sogar gesucht – wird. Meine bisherigen Erfahrungen haben mir darüber hinaus auch gezeigt, dass dieser Rat auch angenommen wird, zwar nicht immer, aber oft genug, was wohl auch auf die Unterstützung des LfD durch die Datenschutzkommission zurückzuführen ist, in der die Fraktionen des Landtags und der Staatssekretär im Innenministerium als Repräsentant der Landesregierung vertreten sind.

Damit bin ich bei der zweiten Ausnahme, die ich von der institutionellen Abfassung des Tätigkeitsberichtes machen möchte. Ich erlaube mir zum Abschluss dieser Vorbemerkung auch ein paar Worte des Dankes. Danken möchte ich den Mitgliedern des Landtags und der Landesregierung für das Vertrauen, das sie mir entgegengebracht haben und noch entgegenbringen, den Mitgliedern der Datenschutzkommission für die Unterstützung meiner Arbeit und meinen Mitarbeitern, die diesen Tätigkeitsbericht nicht nur verfasst, sondern auch die in ihm geschilderten Einzelfälle bearbeitet haben. Ihnen ist es vor allem zu danken, dass der Wechsel im Amt des LfD reibungslos verlaufen ist. Auch der Verwaltung des Landtags, insbesondere dem Personal- sowie Haushaltsreferat, der Druckerei und der Poststelle gilt der besondere Dank für die Unterstützung bei der Wahrnehmung der Verwaltungsaufgaben des LfD.

2. Datenschutz auf der europäischen Ebene

2.1 Aktuelle Entwicklung

Die europäische Rechtsentwicklung ist durch das Ziel geprägt, eine Intensivierung der polizeilichen und justiziellen Zusammenarbeit zu erreichen; man will einen „Raum der Freiheit, der Sicherheit und des Rechts" schaffen. Der Vertrag von Prüm, der inzwischen Teil des Rechts der Europäischen Union geworden ist, soll allen Sicherheitsbehörden der Mitgliedstaaten den Zugriff auf Fingerabdruck-, DNS- und Kraftfahrzeugdaten der anderen Staaten ermöglichen. Europol soll weitere Aufgaben erhalten und nicht nur im Rahmen des Informationsaustauschs Zusammenarbeit praktizieren, sondern auch „operativ" tätig werden können. Das Schengener Informationssystem soll erheblich ausgebaut und erweitert werden; die Planungen werden mit dem Stichwort „SIS II" bezeichnet. Ein europaweites Zollinformationssystem wird aufgebaut. Bei Interpol entsteht eine integrierte Datenbank über vermisste Personen. Die Sicherheitsbehörden sollen Zugriff auf das europäische VISA-Informationssystem (VIS) erhalten. Das europäische Verfahren zur Erfassung von Personen mit ihren Fingerabdrücken – Eurodac – wird vorangetrieben, obwohl Fragen der Datenschutzkontrolle weitgehend ungeklärt sind. Zu Datenschutzdefiziten im Zusammenhang mit der internationalen Zusammenarbeit der Sicherheitsbehörden s. auch unten Tz. 5.14. Die Übermittlung von Flugpassagierdaten in die USA hat in der Öffentlichkeit große Aufmerksamkeit hervorgerufen. Auch hier spielt die EG bei der Schaffung rechtlicher Grundlagen für das Verfahren eine maßgebliche Rolle (s. unten Tz. 2.3). Die europäische und internationale Zusammenarbeit in Strafsachen wird auch auf justizieller Ebene verstärkt; ein europäisches Register der Strafurteile wird geschaffen (bzw. es werden gegenseitige Zugriffsmöglichkeiten auf die nationalen Register erwogen). Alle diese Entwicklungen haben unmittelbare und spürbare Auswirkungen auf die Bürger.

Auf europäischer Ebene gibt es insbesondere folgende Einrichtungen, die im Sinne des Datenschutzes Einfluss ausüben: Die EG-Datenschutzrichtlinie sieht zwei Gremien vor, die den Datenschutz auf europäischer Ebene koordinieren. Das eine ist die Datenschutzgruppe nach Art. 29 der Richtlinie (s. 20. Tb., Tz. 3.3). Diese setzt sich aus den Vertretern der nationalen Kontrollstellen zusammen; für die Bundesrepublik gibt es neben einem Vertreter des BfDI auch ein von den Landesbeauftragten bestimmtes Mitglied. Außerdem entsendet die Kommission einen Vertreter. Daneben existiert der Ausschuss nach Art. 31 der Richtlinie. Dieser unterstützt die Kommission bei der Durchführung der Datenschutzrichtlinie. Ein Vertreter der Kommission führt in ihm den Vorsitz, hat jedoch kein Stimmrecht. Im Übrigen gehören ihm Vertreter der Mitgliedsstaaten an. Der Ausschuss gibt zu jeder von der Kommission geplanten Maßnahme eine Stellungnahme ab. Beide Gremien befassen sich u.a. mit dem Problem der transatlantischen Datenflüsse. Die Entschließungen der Art. 29-Gruppe wurden wiederholt vom europäischen Parlament aufgegriffen und in seine Stellungnahmen einbezogen (s. 21. Tb. des BfDI, S. 31). Allerdings fehlt derzeit noch ein durch eine rechtliche Regelung vorgesehenes unabhängiges Beratungs- und Kontrollorgan für den Bereich der Dritten Säule der EU (dies ist der Bereich von Innerer Sicherheit, Polizei und Justiz). Diese Lücke wird derzeit durch die Arbeitsgruppe Polizei und Justiz der Art. 29-Gruppe eher provisorisch gefüllt. Die Rolle des europäischen Datenschutzbeauftragten muss in diesem Zusammenhang ebenfalls erwähnt werden: er äußert sich engagiert zu Fragen der Rechtsetzung, auch außerhalb seines durch die

ihn betreffenden Rechtsgrundlagen auf den Bereich der Ersten Säule der EU beschränkten Zuständigkeitsbereichs (http://www.edps.europa.eu/EDPSWEB).

2.2 Vertragsverletzungsverfahren der Europäischen Kommission gegen die Bundesrepublik Deutschland

Die öffentlichen Stellen des Bundes sowie die Unternehmen, die geschäftsmäßig Telekommunikations- oder Postdienstleistungen erbringen, unterliegen der Aufsicht durch den Bundesbeauftragten für den Datenschutz. Die Landesbehörden werden durch die Landesdatenschutzbeauftragten kontrolliert. Die privaten Unternehmen (bis auf Telekommunikation und Post) unterliegen der Aufsicht der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die in einigen Bundesländern beim Landesdatenschutzbeauftragten, in anderen Bundesländern bei einer Landesbehörde (in Rheinland-Pfalz bei der Aufsichts- und Dienstleistungsdirektion in Trier) angesiedelt sind. Die EU-Kommission ist der Auffassung, dass Landesdatenschutzbeauftragte und Landesbehörden nicht „in völliger Unabhängigkeit“ arbeiten würden, soweit die jeweilige Landesregierung weisungsbefugt sei.

Die Europäische Kommission hat zu dieser Problematik am 5. Juli 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Dessen Ausgang ist zur Zeit noch ungewiss. In diesem Zusammenhang hat es unterschiedliche Stellungnahmen seitens einiger Datenschutzbeauftragter einerseits, der Bundesregierung andererseits gegeben. Der LfD hat stets die Auffassung vertreten, dass die in der Europäischen Datenschutzrichtlinie geforderte völlige Unabhängigkeit auch dann gewahrt ist, wenn die Datenschutzaufsichtsbehörden der Ministerverantwortung unterliegen. Maßgeblich sei – und insoweit hat er die Auffassung der Bundesregierung geteilt –, dass gegenüber den zu kontrollierenden Stellen eine absolute Unabhängigkeit bestehen müsse. Dies sei aber nach der derzeitigen Rechtslage garantiert.

Einer Übertragung der Aufgabe der Datenschutzkontrolle im privaten Bereich auf die Landesdatenschutzbeauftragten stehen allerdings ebenfalls keine zwingenden Gesichtspunkte entgegen, so dass es sicher überlegenswert ist, den Bedenken der Kommission durch eine Verlagerung der Zuständigkeiten auf die unabhängigen Landesbeauftragten für den Datenschutz Rechnung zu tragen (vgl. auch die Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck, Unabhängige Datenschutzkontrolle in Deutschland gewährleisten, s. Anlage 7).

2.3 Zum Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Fluggastdatensätze

Die Frage, in welchem Umfang Fluggastdaten durch die Luftfahrtunternehmen an amerikanische Sicherheitsbehörden weiterzugeben sind, hat breite öffentliche Aufmerksamkeit gefunden (s. schon 20. Tb., Tz. 3.2). Der LfD will deshalb der Schilderung der aktuellen Situation in diesem Zusammenhang Raum geben.

Das erklärte Ziel des neuen Abkommens ist es, den Terrorismus und das internationale Verbrechen zu verhüten und zu bekämpfen. Einerseits soll eine Rechtsgrundlage für die Übermittlung von Fluggastdatensätzen der Europäischen Union an die USA geschaffen und andererseits ein angemessener Schutz personenbezogener Daten und Verfahrensgarantien für EU-Bürger gewährleistet werden. Es ersetzt die früheren Abkommen über Fluggastdatensätze zwischen der Europäischen Gemeinschaft und den USA vom 28.5.2004 und zwischen der Europäischen Union und den USA vom 19.10.2006. Nach dem neuen Abkommen wird die Zahl der Datenfelder von 34 auf 19 verringert; diese Verringerung dürfte allerdings im Wesentlichen kosmetischer Art sein, da es sich dabei um die Zusammenlegung und Umbenennung von Datenfeldern statt um tatsächliche Streichungen handelt. Sensible Daten (z.B. personenbezogene Daten, die die ethnische Herkunft, politische Meinungen, religiöses Bekenntnis oder Weltanschauung oder die Mitgliedschaft in einer Gewerkschaft offen legen, und Daten betreffend Gesundheit oder sexuelles Verhalten von Personen) sollen dem US-Ministerium für Innere Sicherheit zugänglich gemacht werden, wenn diese Daten auch nur in Ausnahmefällen vom Ministerium für Innere Sicherheit genutzt werden sollen. Die Dauer der Speicherung von Fluggastdaten wird von dreieinhalb Jahren auf 15 Jahre ausgeweitet. Diese Ausweitung soll rückwirkend auch für Daten gelten, die während der Laufzeit der früheren Abkommen über Fluggastdatensätze erfasst wurden. Eine Garantie, dass die Daten nach diesem Zeitraum endgültig gelöscht werden, besteht allerdings nicht. Die Daten sollen sieben Jahre lang in „aktiven Analysedatenbanken“ gespeichert werden. Damit besteht ein erhebliches Risiko massiver Profilerstellung und „Datenausbeute“, was nach Auffassung des Europaparlaments mit den grundlegenden europäischen Prinzipien unvereinbar sei und eine Praxis darstelle, die auch im US-Kongress noch umstritten sei (Entschließung des Europäischen Parlaments vom 12. Juli 2007, BR-Drs. 615/07 vom 28.8.2007).

Es ist die Möglichkeit vorgesehen, dass das Ministerium für Innere Sicherheit Fluggastdaten anderen innerstaatlichen Behörden der USA in besonderen Fällen und in einem Umfang, wie dies der jeweilige Fall erfordert, weitergeben kann. Eine präzise Festlegung, welche US-Behörden Zugang zu den Fluggastdaten bekommen sollen, fehlt. Drittländern soll ganz allgemein der Zugang zu Fluggastdaten möglich sein, sofern sie die vom US-Ministerium für Innere Sicherheit festgelegten Bedingungen erfüllen, und in nicht näher bestimmten Notfällen soll Drittländern ausnahmsweise der Zugang zu Fluggastdaten ermöglicht

werden ohne die Gewähr, dass die Daten entsprechend dem Datenschutzniveau des Ministeriums für Innere Sicherheit verwendet werden. Es soll zulässig sein, analytische Informationen aus den Fluggastdatensätzen durch die US-Behörden an die Polizei und die Justizbehörden in den EU-Mitgliedstaaten und möglicherweise an Europol und Eurojust unabhängig von konkreten Gerichtsverfahren oder polizeilichen Ermittlungen weiterzugeben. Dies sollte aus der Sicht des Datenschutzes aber nur auf der Grundlage der bestehenden Abkommen zwischen der Europäischen Union und den USA über gegenseitige Rechtshilfe und Auslieferung erlaubt sein. Spätestens zum 1.1.2008 soll zumindest grundsätzlich zum Push-System, bei dem das übermittelnde Luftfahrtunternehmen die Übermittlung veranlasst, übergegangen werden. Dieser Übergang, der bereits im Abkommen über Fluggastdatensätze von 2004 vorgesehen war, ist zu begrüßen. Eine gemeinsame regelmäßige Überprüfung durch das US-Ministerium für Innere Sicherheit und die Europäische Union ist vorgesehen. Auch dies ist zu begrüßen. Ein wesentliches datenschutzrechtliches Anliegen ist es, die Fluggäste ordnungsgemäß über die Verwendung ihrer Daten und über ihre Rechte zu informieren, namentlich über die Rechtsbehelfe und darüber, aus welchem Grund ein Fluggast aufgehalten werden kann. Die Kurzinformation für Reisen zwischen der Europäischen Union und den USA, die von der Arbeitsgruppe nach Artikel 29 (AG 132) vorgeschlagen wurde, sollte allen Fluggästen von den Luftfahrtunternehmen zur Verfügung gestellt werden (s. z.B. http://www.lufthansa.com/online/portal/lh/de/info_and_services/partner?l=de&nodeid=1757453).

Insgesamt weist das neue Abkommen wesentliche Mängel auf, was die Rechtssicherheit, den Datenschutz und die Rechtsmittel der EU-Bürger anbelangt, insbesondere wegen der offenen und ungenauen Begriffsbestimmungen und zahlreicher Möglichkeiten für Ausnahmeregelungen. In Übereinstimmung mit der Bewertung des europäischen Parlaments ist auch der LfD der Auffassung, dass der Mangel an demokratischer Kontrolle beim Zustandekommen und bei der Durchführung des Abkommens zu bedauern sind. Das Abkommen ist stark von den amerikanischen Forderungen geprägt und ohne jede Einbeziehung des Europäischen Parlaments ausgehandelt und vereinbart worden. Außerdem wurde auch den nationalen Parlamenten nur unzureichend Gelegenheit geboten, Einfluss auf die Aushandlung zu nehmen oder das vorgeschlagene neue Abkommen eingehend zu prüfen und Änderungen vorzuschlagen.

2.4 Europäisches System zur Erfassung von Fluggastdaten

Das vorgenannte Abkommen erwähnt ein mögliches künftiges Fluggastdaten-Erfassungssystem auf EU-Ebene oder in einem oder mehreren Mitgliedstaaten. Es enthält die Regelung, dass alle Fluggastdaten in einem solchen System dem US-Ministerium für Innere Sicherheit zur Verfügung gestellt werden können. Die Beratungen hinsichtlich eines EU-Fluggastdaten-Erfassungssystems waren bis zum Ende des Berichtszeitraums noch nicht abgeschlossen. Die Arbeitsgruppe nach Artikel 29 hat diesbezüglich Besorgnisse zum Ausdruck gebracht, was die Verwendung der Fluggastdaten zu Zwecken der Strafverfolgung angeht.

Folgendes sollte klargestellt werden:

- die Notwendigkeit und der Zweck der Erfassung von Fluggastdaten bei der Einreise in das Gebiet der Europäischen Union,
- der zusätzliche Nutzen der Erfassung von Fluggastdaten bei der Einreise in die Europäische Union zu Sicherheitszwecken im Lichte der bereits bestehenden Kontrollmaßnahmen, wie dem Schengen-System und dem Visum-Informationssystem,
- die für Fluggastdaten vorgesehene Verwendung, insbesondere ob dies zur Identifizierung von Einzelpersonen zur Gewährleistung der Flugverkehrssicherheit, zur Identifizierung der Personen, die in das Gebiet der Europäischen Union einreisen, oder für das Erstellen von Profilen von Fluggästen geschieht.

Die Richtlinie 2004/82/EG des Rates vom 29.4.2004 geht bereits in diese Richtung. Sie sieht vor, dass Beförderungsunternehmen auf Anforderung der Grenzschutzbehörden bei Flügen aus Drittstaaten in die EU bestimmte Passagierdaten an diese Behörden zu übermitteln haben. In Umsetzung dieser Richtlinie liegt derzeit ein Änderungsentwurf des Bundespolizeigesetzes vor (BT-Drs. 16/6292 v. 4.9.2007). Dieser Entwurf geht über die Anforderungen der Richtlinie hinaus und ist aus Datenschutzsicht kritisch zu sehen. Das Gesetzgebungsverfahren war zum Zeitpunkt der Berichterstellung noch nicht abgeschlossen.

2.5 Der Prümer Vertrag

Der Prümer Vertrag hat zum Ziel, den jeweiligen Polizeibehörden den Direktzugriff auf folgende nationale Datenbestände der beteiligten Staaten zu ermöglichen:

- DNA-Dateien
- Fingerabdruckdateien
- Kraftfahrzeugzulassungsregister

Als zentrale Datenschutzvorkehrung ist für die Abrufe aus den Fingerabdruck- und DNA-Dateien ein zweistufiges Verfahren vorgesehen:

Auf der ersten Stufe wird im Wege des Direktabrufs nur übermittelt, ob ein Treffer, d.h. eine Übereinstimmung mit den übermittelten Vergleichsinformationen, vorliegt (hit/no hit-Verfahren).

Auf der zweiten Stufe werden die weiteren Personendaten auf der Grundlage der bisherigen Rechtshilferegelungen angefordert und übermittelt. Ergänzt wird dies durch detaillierte besondere Datenschutzregelungen, die beispielsweise die Zweckbindung und die Auskunftsrechte der Betroffenen regeln.

Die Abfragen erfolgen sämtlich über das BKA als Zentralstelle. Ursprünglich waren zwölf Staaten Vertragspartner; seit Juni 2007 ist der Vertrag im Wesentlichen Gegenstand eines EU-Ratsbeschlusses geworden, so dass sämtliche 27 Mitgliedsstaaten der EU einbezogen sind. Praktiziert werden kann das Verfahren allerdings erst, wenn die beteiligten Staaten die technischen Vorkehrungen getroffen haben, um die Datenabrufe zu ermöglichen. Derzeit kann das Verfahren also nur zwischen Deutschland, Österreich und Spanien genutzt werden. Allein die damit ermöglichten Abgleiche haben zu erheblichen Erfolgen bei der Straftatenaufklärung geführt.

Aus Datenschutzsicht gibt es insbesondere folgende Prüfansätze:
- Erfolgen die Direktabfragen nur unter den Voraussetzungen, unter denen sie nach nationalem deutschen Recht zulässig sind?
- Erfolgen die im Vertrag vorgesehenen Protokollierungen, wenn ja, wo und unter welchen Auswertungsbedingungen?

Ein besonderes datenschutzrechtliches Problem ergibt sich daraus, dass derzeit auf der Ebene des Bundes in INPOL nicht alle Datenlöschungen von ED-Materialien so erfolgen, wie dies aus der Sicht der Landesdatenschutzbeauftragten gesetzlich vorgegeben ist (s. unten Tz. 5.10). Dieses Problem erhält angesichts der europaweiten Abrufmöglichkeiten eine neue Dimension.

Der LfD wird sich um dieses Verfahren mit besonderer Aufmerksamkeit kümmern.

2.6 INSPIRE – Basis einer neuen Geodateninfrastruktur

Seit dem 1.5.2007 ist die Richtlinie zur „Schaffung einer Raumdateninfrastruktur in der Gemeinschaft – INSPIRE“ (INSPIRE = Infrastructure for Spatial Information in Europe) in Kraft getreten (Richtlinie zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) – Richtlinie 2007/2/EG des europäischen Parlaments und des Rates vom 14. März 2007; Fundstelle im Internet: http://www.bmu.de/umweltinformation/geoinformationen/doc/36544.php). Damit sind die Voraussetzungen für den Aufbau einer europäischen Geodateninfrastruktur geschaffen worden. Ziel der Richtlinie ist es, Geodaten aus den Behörden der Mitgliedstaaten unter einheitlichen Bedingungen „zur Unterstützung der Formulierung, Umsetzung und Bewertung europäischer und nationaler Politikfelder“ zugänglich zu machen.

Zur Umsetzung der INSPIRE-Richtlinie wird derzeit ein Bundesgesetz, das „Geodateninfrastrukturgesetz“ (GDIG), erarbeitet. Dieses Gesetz soll innerhalb der kommenden zwei Jahre die rechtlichen Rahmenbedingungen schaffen, um die Geodaten öffentlicher Stellen einfach und standardisiert den Bürgerinnen und Bürgern, der Wirtschaft, der Wissenschaft und der Verwaltung verfügbar zu machen. Zu diesem Zweck ist außerdem durch die Vermessungsverwaltungen eine spezielle technische Infrastruktur (mit dem Arbeitstitel „Geodateninfrastruktur in Deutschland; GDI-DE“) zu entwickeln. Für Daten von Länderbehörden werden Landesgesetze erforderlich sein. Die Gesetze sollen Geodaten verschiedener Verwaltungsbereiche, die auch Personenbezug haben können, betreffen. Das Geodateninfrastrukturgesetz des Bundes wird den Ländern sicherlich als Vorlage mit Vorbildfunktion dienen.

Da diese Gesetze und die zugrundeliegende EG-Richtlinie keine geringe datenschutzrechtliche Bedeutung haben, hat der LfD angeregt, die Entwicklung auf diesem Gebiet in der Unterarbeitsgruppe „Geodaten“ der Konferenz der Datenschutzbeauftragten zu thematisieren. Er wird diese Gesetzgebungsaktivitäten insbesondere auf der Ebene des Landes frühzeitig begleiten. Das ISM hat bereits angekündigt, ihn aktiv und umfassend zu informieren.

2.7 Der Zugriff amerikanischer Sicherheitsbehörden auf europäische Bankdaten – die „SWIFT“-Affäre

SWIFT ist ein weltweit agierender Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen. Dessen datenschutzrelevantes Kennzeichen ist, dass sämtliche internationalen Überweisungsdaten für 124 Tage nicht nur im Rechenzentrum von SWIFT in Belgien, sondern zu Datensicherungszwecken auch vollständig in den USA in einem anderen SWIFT gehörenden Rechenzentrum (als gespiegelter Datensatz) gespeichert werden. Dort haben die US-Sicherheitsbehörden grundsätzlich den Zugang, den sie zu allen in den USA gespeicherten Daten haben. Nach den Terrorangriffen vom September 2001 verlangte das US-Finanzministerium von SWIFT Zugang zu den in den USA gespeicherten Daten. Aufgrund von Presseberichten Ende Juni/Anfang Juli 2006 erfuhr die Öffentlichkeit erstmals von dieser Angelegenheit. Inzwischen bestehen

Vereinbarungen zwischen der US-Regierung und SWIFT, die Zweckbindungsregelungen, Kontrollrechte von SWIFT und andere Maßnahmen der Eingriffsbeschränkung umfassen. Die Zahlungsanweisungen enthalten personenbezogene Daten wie Namen des Zahlungsanweisenden und des Zahlungsempfängers. SWIFT unterliegt als in Belgien gelegene Kooperative belgischem Recht, das die EG-Datenschutzrichtlinie umsetzt. Die Finanzinstitute in der EU, die die Dienstleistungen von SWIFT benutzen, unterliegen den jeweiligen nationalen Datenschutzvorschriften in den Ländern, in denen sie angesiedelt sind.

Die deutschen obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich („Düsseldorfer Kreis") haben am 8./9.11.2006 in Bremen über das SWIFT-Verfahren beraten. Sie haben einmütig einen Beschluss (zugänglich im Internetangebot des BfDI http://www.bfdi.bund.de/cln_029/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/Functions/DKreis__table.html) gefasst, in dem sie die USA zu einem Staat ohne angemessenes datenschutzrechtliches Schutzniveau erklären mit der Folge, dass eine Datenverarbeitung dort nur dann zulässig wäre, wenn sichergestellt würde, dass kein staatlicher Zugriff auf die übermittelten Daten erfolgen könnte. Dies könne etwa durch eine wirksame Verschlüsselung erreicht werden. Wörtlich heißt es in diesem Beschluss:

„Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie." Die Datenübermittler „werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren."

Die in der sog. Art. 29-Datenschutzgruppe organisierten europäischen Datenschutzbeauftragten haben in einer Presseerklärung vom 23.11.2006 zu der SWIFT Affäre u.a. folgendes erklärt (Abrufbar im Internet unter dem Angebot der Europäischen Kommission: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm):

SWIFT und die Finanzinstitute in der EU hätten die Vorgaben der Richtlinie nicht beachtet. Hinsichtlich der Verarbeitung und der Spiegelung personenbezogener Daten im Rahmen des SWIFTNet FIN Services hätte SWIFT seinen Verpflichtungen nach der Richtlinie als der für die Verarbeitung verantwortlichen Stelle nachkommen müssen; dies betreffe insbesondere die Informationspflicht, die Meldepflicht, die Verpflichtung zur Wahrung eines angemessenen Schutzniveaus bei internationalen Datentransfers. Die Finanzinstitute in der EU hätten als die für die Verarbeitung von personenbezogenen Daten verantwortlichen Stellen die rechtliche Verpflichtung, sicherzustellen, dass SWIFT vollständig die rechtlichen Anforderungen, insbesondere auch des Datenschutzrechts, erfüllt, um den Schutz ihrer Kunden zu gewährleisten. Den Finanzinstituten hätte auch oblegen, sich hinreichende Kenntnisse über die unterschiedlichen Zahlungssysteme und deren technische und rechtliche Ausgestaltung und Risiken zu verschaffen: Wenn und soweit Finanzinstitute sich nicht (hinreichend) bemüht haben sollten, diese Kenntnisse zu erlangen, hätten sie wesentliche rechtliche Risiken hinsichtlich ihrer grundlegenden Sorgfaltspflichten gegenüber ihrer Kunden in Kauf genommen. Die Art. 29-Gruppe hält es für unabdingbar, dass die einzelnen Kunden der Finanzinstitute in Übereinstimmung mit den Transparenzforderungen der Richtlinie durch die Finanzinstitute als deren professionelle Dienstleister hinreichend unterrichtet werden. Weiter vertritt die Artikel 29-Gruppe die Auffassung, dass der Mangel an Transparenz sowie an angemessenen und effektiven Kontrollmechanismen, der den gesamten Prozess der Übermittlung von personenbezogener Daten in die USA und weiter an das US-Finanzministerium präge, eine schwere Verletzung der Richtlinie darstelle. Darüber hinaus seien auch die Garantien für die Datenübermittlung in ein Drittland, so wie sie die Richtlinie vorsehe, und die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit nicht beachtet worden.

Das konkrete Vorgehen von SWIFT bei der Datenüberlassung an die US-amerikanischen Sicherheitsbehörden und das Zusammenwirken mit diesen sei insbesondere wegen der unterlassenen Information der Kunden und der Mitgliedsbanken durch SWIFT als konkreter vorwerfbarer Verstoß gegen europäisches Datenschutzrecht zu werten.

Nach Auffassung des LfD ist das Problem bislang noch nicht zufriedenstellend gelöst. Zwar werden die Bankkunden inzwischen auf die Zugriffsmöglichkeiten der US-Behörden hingewiesen. Datenschutzpolitisch muss aber ein Weg gesucht werden, um die – zu Recht – als unakzeptabel und als nicht hinnehmbar empfundene Totalüberwachung des internationalen Überweisungswesens durch die US-amerikanischen Sicherheitsbehörden künftig zu verhindern. Ein Verfahren zur Lösung solcher Probleme sieht Art. 25 Abs. 3 bis 6, Art. 26 Abs. 2 EGDSRL mit Erwägungsgrund 59 ausdrücklich vor. Voraussetzung dafür ist ein entschlossenes Handeln der Regierungen auf europäischer Ebene.

Zu den in Rheinland-Pfalz erfolgten Aktivitäten gegenüber den öffentlich-rechtlichen Kreditinstituten des Landes s. Tz. 22.3.

3. Datenschutz auf der Ebene des Bundes

Einen wichtigen Teil der Tätigkeiten des LfD haben Stellungnahmen zu Vorgängen eingenommen, die auf der Ebene des Bundes zu entscheiden waren, sei es im Rahmen des Gesetzgebungsverfahrens oder im Zusammenhang mit Verfahren vor dem Bundesverfassungsgericht. So war der LfD insbesondere an den Diskussionen im Rahmen des Gesetzgebung des Bundes beteiligt, die aus seiner Sicht zu wesentlichen Auswirkungen auf die Datenverarbeitung von Landesstellen führen würden, angefangen beim Sicherheitsbereich (z.B. den Neuregelungen der Strafprozessordnung, s. unten Tz. 7.1) über den Bereich der Geodaten (s. oben Tz. 2.6) bis hin zum Steuer- und Abgabenrecht (s. unten Tz. 13.3). Diese Beispiele sollen für einen Teil der behandelten Bundesthemen stehen; wie umfangreich die hier zu nennenden Aktivitäten sind, wird im Bericht an zahlreichen Stellen deutlich.

In diesem Zusammenhang geht es zum einen und vor allem darum, die Landesregierung vor ihren Abstimmungen im Bundesrat zu beraten; wichtig ist aber auch, bei der gemeinsamen Meinungsbildung der Datenschutzbeauftragten des Bundes und der Länder rechtzeitig informiert zu sein, um angemessen mitwirken zu können. Schließlich erleichtert eine Einbindung in die Phase der Entstehung eines Gesetzes auch die Mitwirkung bei dessen praktischer Umsetzung durch Landesstellen. Vor diesem Hintergrund hält es der LfD für erforderlich, dass er rechtzeitig von der Landesregierung bzw. den jeweils zuständigen Ministerien über entsprechende Gesetzesvorhaben unterrichtet wird. Eine solche Unterrichtung findet häufig nicht oder nicht rechtzeitig statt. Derzeit werden Gespräche geführt, um effiziente Verfahren zu vereinbaren, die dieses Ziel fördern.

Sehr zu begrüßen ist aus der Sicht des LfD die Übung des Bundesverfassungsgerichts, neben dem Bundesdatenschutzbeauftragten allen Landesdatenschutzbeauftragten die Gelegenheit zur Stellungnahme zu geben, wenn Verfahren von grundsätzlicher datenschutzrechtlicher Bedeutung anstehen. Von dieser Möglichkeit der Stellungnahme macht der LfD insbesondere dann Gebrauch, wenn das jeweils verhandelte datenschutzrechtliche Anliegen aus seiner Sicht verfassungsrechtlich begründet ist. An dieser Stelle ist die positive Rolle hervorzuheben, die das Bundesverfassungsgericht bei der Fortentwicklung und Durchsetzung des Datenschutzes spielt. Nur beispielhaft sei auf folgende Entscheidungen hingewiesen, die im Berichtszeitraum gefällt worden sind:

- Erfolgreiche Verfassungsbeschwerde eines im Maßregelvollzug Untergebrachten gegen die Verweigerung der Einsicht in seine Krankenunterlagen, Beschluss vom 9.1.2006 – 2 BvR 443/02 –
- Recht auf informationelle Selbstbestimmung schützt im Herrschaftsbereich des Teilnehmers gespeicherte Telekommunikationsverbindungsdaten; Urteil vom 2.3.2006 – 2 BvR 2099/04 –
- Behördliches Auskunftsverlangen über Wiedererwerb der türkischen Staatsangehörigkeit verfassungsrechtlich nicht zu beanstanden; Beschluss vom 10.3.2006 – 2 BvR 434/06 –
- Rasterfahndung nur bei konkreter Gefahr für hochrangige Rechtsgüter zulässig; Beschluss vom 4.4.2006 – 1 BvR 518/02 –
- Persönlichkeitsschutz bei der Verbreitung von Luftaufnahmen der Anwesen Prominenter; Beschluss vom 2.5.2006 – 1 BvR 507/01 –
- Bundesverfassungsgericht rügt vorschnelle Wohnungsdurchsuchung bei unzureichender Verdachtsgrundlage; Beschluss vom 3.7.2006 – 2 BvR 2030/04 –
- Gerichtlicher Durchsuchungs- oder Abhörbeschluss muss Mindestmaß an Darlegungsanforderungen erfüllen; Beschluss vom 4.7.2006 – 2 BvR 950/05 –
- Erfolglose Verfassungsbeschwerde im Zusammenhang mit einer Bildberichterstattung über eine Privatperson ohne hervorgehobene Prominenz; Beschluss vom 21.8.2006 – 1 BvR 2606/04; 1 BvR 2845/04; 1 BvR 2846/04; 1 BvR 2847/04 –
- Ermittlung von Mobilfunkdaten durch IMSI-Catcher verstößt nicht gegen Grundrechte; Beschluss vom 22.8.2006 – 2 BvR 1345/03 –
- Gerichtlicher Durchsuchungsbeschluss muss Mindestmaß an Darlegungsanforderungen erfüllen; Beschluss vom 7.9.2006 – 2 BvR 1219/05 –
- Durchsuchung einer Anwaltskanzlei wegen Parkverstoßes unverhältnismäßig; Beschluss vom 7.9.2006 – 2 BvR 1141/05 –
- Verfassungswidrigkeit einer Wohnungsdurchsuchung bei Tage ohne richterliche Anordnung und unter Einsatz eines Drogenspürhundes; Beschluss vom 28.9.2006 – 2 BvR 876/06 –
- Versicherungsvertragliche Obliegenheit zur Schweigepflichtentbindung muss Möglichkeit zu informationellem Selbstschutz bieten; Beschluss vom 23.10.2006 – 1 BvR 2027/02 –
- Der Beschwerdeführer wandte sich gegen ein zivilgerichtliches Urteil, durch das eine Klage auf sofortige Löschung von Telekommunikationsverkehrsdaten nach Ende der Verbindung abgewiesen wurde. Seiner Beschwerde wurde stattgegeben; Beschluss vom 27.10.2006 – 1 BvR 1811/99 –
- Heimlicher Vaterschaftstest darf im gerichtlichen Verfahren nicht verwertet werden – Gesetzgeber muss aber Verfahren allein zur Feststellung der Vaterschaft bereitstellen; Urteil vom 13.2.2007 – 1 BvR 421/05 –
- Durchsuchung und Beschlagnahme bei CICERO verletzen Pressefreiheit; Urteil vom 27.2.2007 – 1 BvR 538/06; 1 BvR 2045/06 –

- Städtische Videoüberwachung eines Kunstwerks in Regensburg entbehrt gesetzlicher Grundlage; Beschluss vom 23.2.2007 – 1 BvR 2368/06 –
- Erfolgreiche Verfassungsbeschwerde eines Strafverteidigers gegen die Überwachung seines Mobiltelefonanschlusses; Beschluss vom 18.4.2007 – 2 BvR 2094/05 –
- Erfolgreiche Verfassungsbeschwerde des Anwalts von El Masri gegen die Überwachung seines Telefons, weil die Wahrscheinlichkeit, dass relevante Erkenntnisse gewonnen werden könnten, von vornherein so gering war, dass die Erfolgsaussichten der Maßnahme außer Verhältnis zur Schwere des Eingriffs standen; Beschluss vom 30.4.2007 – 2 BvR 2151/06 –
- Die Regelungen zur akustischen Wohnraumüberwachung in der StPO sind verfassungskonform; Beschluss vom 11.5.2007 – 2 BvR 543/06 –
- Vorschriften zum automatischen Kontenabruf verstoßen teilweise gegen den verfassungsrechtlichen Bestimmtheitsgrundsatz; Beschluss vom 13.6.2007 – 1 BvR 1550/03; 1 BvR 2357/04; 1 BvR 603/05 –

Mit diesen Entscheidungen hat das Bundesverfassungsgericht maßgebliche Beiträge im Sinne des Datenschutzes geleistet. Dem Bundesverfassungsgericht kommt bei der Gewährleistung des Rechts auf informationelle Selbstbestimmung in soweit eine besonders wichtige Bedeutung zu.

Im Zusammenhang mit dem Datenschutz auf Bundesebene muss schließlich die Tätigkeit des BfDI gewürdigt werden. Er hat mit seinem unermüdlichen Einsatz und dem Engagement seiner sachkundigen und motivierten Mitarbeiter wesentlichen Anteil daran, dass dem Datenschutz Gehör geschenkt wird. Seine detaillierten und umfassenden Tätigkeitsberichte, die im Internet zur Verfügung stehen, sind Belege dafür. Insbesondere bei der Gesetzgebung existieren vielfältige Berührungspunkte zwischen Landes- und Bundeskompetenzen. Deshalb ist eine enge Zusammenarbeit zwischen den Landesbeauftragten und dem BfDI unerlässlich; diese wird vom BfDI in dankenswerter Weise gepflegt.

4. Meldewesen

4.1 Änderungen im Betrieb des Einwohnerinformationssystems Rheinland-Pfalz EWOIS

Der technische Betrieb des Einwohnerinformationssystems Rheinland-Pfalz wurde im Berichtszeitraum neu ausgeschrieben. Neben einem Wechsel des Betreibers zentraler Komponenten sind dabei auch konzeptionelle Änderungen erfolgt, für die der LfD im Vorfeld der Ausschreibung um eine neuerliche datenschutzrechtlichen Bewertung gebeten wurde. Im Wesentlichen betraf dies den künftigen Betrieb des Kommunalen Netzes Rheinland-Pfalz als zentrales Zugangsnetz der Kommunen und Landesverwaltungen zu den einzelnen EWOIS-Komponenten.

Mit Blick auf die seinerzeitige Übernahme wesentlicher Betriebsaufgaben des EWOIS-Verfahrens durch eine nicht-öffentliche Stelle hatte der LfD in seinem 19. Tätigkeitsbericht auf die Notwendigkeit hingewiesen, den Wegfall aufsichtlicher Einwirkungsmöglichkeiten durch eine geeignete Vertragsgestaltung und technisch-organisatorische Maßnahmen zu kompensieren (19. Tb., Tz. 21.2.5.5). Mit Blick auf die damalige Ausgestaltung des Kommunalnetzes als logisches Teilnetz des rlp-Netzes hatte er hierzu empfohlen, die Steuerung und Kontrolle der Verbindungswege in der Hand einer der Aufsicht des Landes unterstehenden Stelle zu belassen. Dem wurde entsprochen, indem die Administration der Kommunikationswege für Verbindungen zwischen dem rlp-Netz und dem Kommunalnetz, der Betrieb einer Firewall am Übergang des Kommunalen Netzes zum Rechenzentrum des EWOIS-Betreibers sowie der Betrieb der Netzkomponenten bei den Teilnehmern des Kommunalnetzes in die Verantwortung des LDI gelegt wurde (Tz. 21.2.5.6). Dieser war, eine Besonderheit der damaligen Anbieterkonstellation, einerseits Subunternehmer des auftragnehmenden Konsortiums und hatte andererseits für dieses bei zentralen Aufgaben des Netzmanagements gleichzeitig Aufsichtsfunktionen. Um eine wirksame Wahrnehmung der Kontroll- und Steuerungsaufgaben zu gewährleisten, wurde der LDI in diesen Bereichen gegenüber dem Betreiber des EWOIS-Verfahrens weisungsfrei gestellt.

Im Unterschied zur damaligen Situation wird das Kommunale Netz künftig als eigenständiges, von der technischen Struktur des rlp-Netzes losgelöstes Netz betrieben. Neben technischen Änderungen ergibt sich daraus eine eindeutige Trennung der Verantwortungsbereiche der jeweiligen Netzbetreiber. Diese liegen für das rlp-Netz beim LDI, für das Kommunale Netz bei der KommWis GmbH als der von den Kommunalen Spitzenverbänden beauftragten Stelle. Die geänderte Konzeption lässt die geforderte Kontrolle der Kommunikationswege für Verbindungen zwischen dem rlp-Netz und dem Kommunalnetz unberührt. Am Übergang des Kommunalnetzes zum rlp-Netz wird auch künftig – in gemeinsamer Verantwortung des LDI und der KommWis GmbH – eine Firewall betrieben, welche die Zulässigkeit von Verbindungen ins Landesnetz und zu dort erreichbaren zentralen Anwendungen steuert. Eine vergleichbare Steuerung erfolgt im Auftrag der KommWis GmbH durch die KDZ am dortigen Übergang zum technischen Betreiber der EWOIS-Systeme.

Die Steuerung und Kontrolle der Netzübergänge liegt damit jeweils in der Hand einer aufsichtlichen Weisungen zugänglichen, öffentlichen Stelle, so dass aus Sicht des LfD die notwendigen Einwirkungsmöglichkeiten erhalten blieben.

Inhaltliche Änderungen ergeben sich durch das neue Betriebskonzept bei der Administration der Netzzugangskomponenten der Teilnehmer. Bereits im Jahr 2005 war hier aus betrieblichen Gründen eine Aufteilung der administrativen Aufgaben erfolgt, indem die Verwaltung der eigentlichen Netzknoten dem technischen Betreiber übertragen wurde. Datenschutzrechtliche Aspekte blieben davon weitgehend unberührt, da dem LDI weiterhin die Administration der hiervon separaten Verschlüsselungsgeräte oblag (vgl. 20. Tb., Tz. 21.2.2). Bei der technischen Neukonzeption des Kommunalen Netzes wurde aus Kostengründen sowie aus betrieblichen Überlegungen jedoch eine gerätemäßige Trennung in Netz- und Verschlüsselungskomponenten aufgegeben. Dies hatte zur Folge, dass Betrieb und Verwaltung der Netzzugangsgeräte nunmehr vollständig dem technischen Betreiber des Kommunalnetzes obliegen. Aus Sicht des LfD mussten angesichts der weiterhin vorgesehenen Anbindung des Kommunalnetzes an das rlp-Netz und die Bereitstellung zentraler Anwendungen des LDI für die Kommunen dem fachlich verantwortlichen Netzbetreiber (KommWis GmbH) auch weiterhin wirksame Kontrollmöglichkeiten verbleiben.

Hierzu ist vorgesehen, dass die für die Authentifizierung der Netzknoten erforderlichen kryptografischen Zertifikate im Auftrag der KommWis GmbH durch die KDZ erstellt und ausgegeben werden. In Verbindung mit der dort betriebenen Firewall kann damit gewährleistet werden, dass nur verlässlich authentifizierte Komponenten Verbindungen im Kommunalnetz und zum rlp-Netz herstellen können. Damit sind weiterhin angemessene Steuerungs- und Kontrollmöglichkeiten gegeben.

Mit der künftig eigenständigen Infrastruktur des Kommunalnetzes liegt eine Situation vor, wie sie vergleichbar für andere an das rlp-Netz angeschlossene Netze (TESTA-Netz, Corporate Network Polizei) sowie in ähnlicher Weise mit Blick auf die lokalen Netze angeschlossener Verwaltungen besteht. Inwieweit diese als vertrauenswürdig angesehen werden können, bemisst sich nach dem Sicherheitskonzept des jeweiligen Netzes bzw. ergänzender Vereinbarungen der Netzbetreiber bzw. Teilnehmer. Angesichts der Situation, dass bei aktuellen Großverfahren Zahl und Vielfalt der eingebundenen Stellen ein zentrales Sicherheitsmanagement oftmals nicht mehr zulassen, besteht aus Sicht des LfD die Notwendigkeit, auf der Grundlage vereinbarter Sicherheitsstandards Verantwortungsbereiche an den Kontroll- und Einwirkungsmöglichkeiten der Beteiligten auszurichten.

Sowohl für das rlp-Netz als auch für das Kommunalnetz ist ein Sicherheitsniveau nach den Vorgaben des BSI-Grundschutzhandbuchs vorgegeben, wodurch grundsätzlich für jedes beteiligte Netz ein Betrieb unter angemessenen Sicherheitsbedingungen gewährleistet werden kann. Darüber hinaus hat der LfD mit Blick auf die Anbindung der beiden Netze eine Vereinbarung der Betreiber angeregt, die eine Abgrenzung der zu verantwortenden Sicherheitsbereiche vornimmt, zusichert, dass Teilnehmeranschlüsse nur nach den Vorgaben des jeweiligen Netzbetreibers eingerichtet werden und festlegt, dass netzübergreifende Verbindungen nur auf der Grundlage einer verlässlichen Authentifizierung der teilnehmenden Stelle zugelassen werden.

4.2 Auswertung der Nutzung des EWOIS-Verfahrens

Um eine effektive Datenschutzkontrolle zu ermöglichen, hatte der LfD im zurückliegenden Berichtszeitaum empfohlen, anstelle einer stichprobenweisen Erfassung zumindest für den Bereich der Gruppenabfragen, d.h. bei Abfragen über eine Vielzahl namentlich nicht näher bezeichneter Personen, grundsätzlich eine vollständige Protokollierung vorzusehen (vgl. 20. Tb. Tz. 21.2.4.2). Dem wurde seinerzeit entsprochen. Im aktuellen Berichtszeitraum hat der LfD anhand dieser Protokollierungen Art und Struktur der EWOIS-Nutzung bei Gruppenabfragen untersucht. Ein Abruf ist in diesen Fällen nur zulässig, soweit dies zur Erfüllung der Aufgaben der abrufberechtigten Stelle erforderlich ist; diese trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs. Aufgrund der Privilegierung der gruppenabfrageberechtigten Stellen ist, um eine effektive Kontrolle zu ermöglichen, für diese Abfrageform vorgesehen, in einem Pflichtfeld den Anfragegrund so konkret zu bezeichnen, dass eine Rückführung auf den jeweils zugrundeliegenden Vorgang möglich ist; in der Regel soll dies durch die Angabe eines Aktenzeichens erfolgen.

Bei einer Kontrolle des LfD zur EWOIS-Nutzung hat sich ergeben, dass im Zeitraum von Januar bis April 2006 insgesamt ca. 320.000 Gruppenabfragen vorgenommen wurden. In etwa 10 % der Fälle wurden dabei erkennbar unsinnige Angaben für den Grund der Abfrage gemacht. Zumeist handelte es sich um Zeichenfolgen, denen wahllose Tastatureingaben zugrunde liegen (qwert, asdf, xyz, ...) oder bei denen Zeichen wiederholt wurden (xxxxxxx, vdfdf, ...). Zum Teil wurden Gründe angegeben, bei denen fraglich blieb, ob es sich um gezielte Provokationen oder Gleichgültigkeit handelte (z.B. „neugier“, „ich“, „ohne“, „egal“, „depp“, „doof“ oder „Durchgeknallter“, „Irrer“ und „Vollsauf“). Aus Sicht des LfD entbehrte dieses Verhalten der notwendigen Sensibilität im Umgang mit dem Instrument der Gruppenabfrage und begründete Zweifel an einer ordnungsgemäßen Nutzung des Verfahrens.

Bei einem Teil der Abfragen haben sich weitere Auffälligkeiten ergeben. Es handelte sich um Abfragen, die nach Art der gewählten Suchkriterien Anlass für Nachfragen gaben (z.B. Abfragen ohne konkrete Anschrift, lediglich mit Vornamen und

Ort; Abfrage bestimmter Geburtsjahrgänge in einzelnen Orten, die Recherche eines einzelnen Namens aus dem Kreis aller 16- bis 23-jährigen im Kreisgebiet oder Abfragen auf bekannte Persönlichkeiten).

Der LfD hat in allen Fällen die betroffenen Verwaltungen gebeten, den Hintergrund der jeweiligen Abfragen zu klären. Soweit mit besonderer Häufigkeit die Angabe aussagekräftiger Gründe unterblieben war, sollte dies erläutert werden. Für die weitere Nutzung des Informationssystems hat er empfohlen, als Grund der Abfrage jeweils das Aktenzeichen, die Bearbeitungsnummer oder eine vergleichbare Angabe einzutragen. Soweit dies im Einzelfall nicht möglich sein sollte, sollte eine Angabe gemacht werden, die den Grund der Abfrage hinreichend kennzeichnet.

Seitens der angesprochenen Verwaltungen konnte für den Großteil der Abfragen, die durch die Art der Suchkriterien zunächst aufgefallen waren, die dienstliche Notwendigkeit nachvollziehbar dargelegt werden. Auch wenn sich im Rahmen der Kontrolle des LfD keine Anhaltspunkte dafür ergeben haben, dass den Betroffenen persönliche Nachteile entstanden sind, blieben in einer nennenswerten Zahl von Fällen Fragen offen. Aus Sicht des LfD muss in der Gesamtschau davon ausgegangen werden, dass bei derartigen Auskunftssystemen ein Bodensatz an missbräuchlichen Abfragen nicht ausgeschlossen werden kann. Diese Erkenntnisse aus der Kontrolle unterstreichen nach seiner Auffassung erneut die Bedeutung einer aussagekräftigen Protokollierung für eine effektive Datenschutzkontrolle. Angesichts der Komplexität heutiger IT-Verfahren bedarf es grundsätzlich einer angemessenen Protokollierung, um die Nutzung der Verfahren transparent zu machen; dies gilt in besonderem Maß dann, wenn umfangreiche Datenbestände betroffen sind und flexible Auswertungsmöglichkeiten bestehen.

Die Aufklärungsbemühungen des LfD wurden seitens des Innenministeriums in vorbildlicher Weise unterstützt. In mehreren Fällen wurden aufgrund der festgestellten Art oder Häufigkeit fragwürdiger Abfragen Dienstordnungsverfahren gegen die jeweiligen Mitarbeiter eingeleitet.

Eine Folgekontrolle des LfD im Jahr 2007 ergab keine Gründe für eine Beanstandung. Der LfD wird seine Kontrollen in diesem Bereich fortsetzen.

5. Polizei

5.1 Vorbemerkung

Im Berichtszeitraum wurde das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz (POG) nicht geändert. Die technische Entwicklung in der polizeilichen Datenverarbeitung schreitet allerdings stetig voran. Die Einbeziehung des Landesbeauftragten für den Datenschutz in die Planungen neuer Systeme und Verfahren ist ausnahmslos frühzeitig erfolgt; er wurde umfassend unterrichtet und hat dabei jeweils die Gelegenheit erhalten (und auch genutzt), seine Auffassung darzulegen.

Insbesondere auf der Ebene des Ministeriums, aber auch im nachgeordneten Bereich hat sich das traditionell erfreulich positive Arbeitsklima im Berichtszeitraum erhalten. Auch im Fall von gelegentlich unterschiedlichen Bewertungen in Detailfragen wurde die sachliche und grundsätzlich auf gegenseitiges Verständnis abzielende Grundhaltung der Diskussion nie aufgegeben.

Der von Gesetzes wegen (gem. § 29 Abs. 12 POG) zu erstattende Bericht des Innenministeriums an das Parlament über den Einsatz der akustischen Wohnraumüberwachung und der Telekommunikationsüberwachung nach dem POG (Bericht über den Einsatz technischer Mittel nach §§ 29, 31 POG für das Jahr 2006, LT-Drs. 15/1502 v. 13. 09. 2007) zeigt, dass diese aus datenschutzrechtlicher Sicht besonders intensiven Eingriffsmaßnahmen nur sehr zurückhaltend angewandt werden.

5.2 Die akustische Wohnraumüberwachung gem. § 29 POG

5.2.1 Entscheidung des rheinland-pfälzischen VGH

Der VGH Rheinland-Pfalz hat die Frage entschieden, ob die Neuregelung der akustischen und optischen Wohnraumüberwachung in § 29 POG mit der Landesverfassung in Einklang steht (Urteil aufgrund der mündlichen Verhandlung vom 29.1.2007, Az.: VGH B 1/06). Durch Gesetz vom 25.7 2005 hatte der rheinland-pfälzische Landtag eine Neufassung der im Jahr 2003 in § 29 POG geschaffenen Regelung über die akustische und optische Wohnraumüberwachung zu präventiven Zwecken, d.h. zu Zwecken der vorbeugenden Gefahrenabwehr, verabschiedet. Die Neufassung sollte die Rechte der Betroffenen insbesondere durch besondere Vorkehrungen zum Schutz des Kernbereichs der persönlichen Lebensgestaltung stärken. Mit seiner hiergegen erhobenen Verfassungsbeschwerde machte der Beschwerdeführer geltend, auch die Neuregelung sei

verfassungswidrig. Insgesamt verletze die in Rede stehende polizeiliche Eingriffsbefugnis sein Grundrecht auf Unverletzlichkeit der Wohnung gemäß Art. 7 Abs. 1 der LV. Er werde in seiner Menschenwürde beeinträchtigt, weil die angegriffene Regelung den absoluten Kernbereich privater Lebensgestaltung nicht ausreichend schütze. Der LfD, der vom VGH zur Stellungnahme aufgefordert worden war, erachtete § 29 POG in der 2005 verabschiedeten Neufassung für datenschutzkonform.

Der rheinland-pfälzische VGH entschied, dass die angegriffene Regelung nicht gegen das Grundrecht der Unverletzlichkeit der Wohnung verstößt. Zwar schütze Art. 7 Abs. 1 LV den elementaren Lebensraum der eigenen Wohnung und gewährleiste das Recht, in ihm in Ruhe gelassen zu werden. Die Regelung enthalte daher das grundsätzliche Verbot, gegen den Willen des Wohnungsinhabers in die Wohnung einzudringen oder Abhörgeräte bzw. Kameras zu installieren. Jedoch ermächtige Art. 7 Abs. 3 LV den Gesetzgeber, die Unverletzlichkeit der Wohnung zur Behebung öffentlicher Notstände einzuschränken. Dies gelte nicht nur im Hinblick auf Naturkatastrophen oder allgemeine Notlagen, wie es der Beschwerdeführer angenommen hatte, sondern berechtige auch zu Maßnahmen der präventiven Wohnraumüberwachung. Allerdings müsse Art. 7 Abs. 3 LV in grundrechtsfreundlicher Auslegung mit dem Schutzniveau in Einklang gebracht werden, das die bundesverfassungsrechtliche Regelung des Art. 13 Abs. 4 GG vermittele. Danach seien Maßnahmen der Wohnraumüberwachung nur zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, und nur auf Grund richterlicher Anordnung gestattet. Bei einer Gesamtschau der gestatteten Grundrechtseingriffe, der strengen Eingriffsvoraussetzungen und zusätzlicher grundrechtssichernder Verfahrensbestimmungen genüge § 29 POG diesen Anforderungen an die Beschränkung des Grundrechts der Unverletzlichkeit der Wohnung.

So sei die Anordnung von Wohnraumüberwachungsmaßnahmen nach § 29 POG erst dann zulässig, wenn der Eintritt dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, hinreichend wahrscheinlich sei. Das Erfordernis der Dringlichkeit der Gefahr für die genannten Rechtsgüter erhöhe nochmals die Eingriffsschwelle sowohl hinsichtlich der Rechtsgüter, deren Schutz die Wohnraumüberwachung dienen solle, als auch des Grades der Wahrscheinlichkeit ihrer Gefährdung. Die zusätzliche Benennung der „gemeinen Gefahr“, die an das Betroffensein einer unbestimmten Zahl von Personen oder Sachen anknüpfe, und der „Lebensgefahr“ gewährleiste, dass nur hochrangige Rechtsgüter eine Wohnraumüberwachung rechtfertigen könnten. Verfahrensrechtlich unterliege die automatische Datenerhebung außerdem einer ständigen begleitenden richterlichen Kontrolle.

§ 29 POG gewährleiste darüber hinaus den absoluten Schutz des unantastbaren Kernbereichs privater Lebensgestaltung. Die Privatwohnung stelle insoweit als „letztes Refugium“ ein Mittel zur Wahrung der Menschenwürde dar. Eine akustische oder optische Wohnraumüberwachung habe deshalb grundsätzlich zu unterbleiben, wenn sich jemand allein oder ausschließlich mit Personen in der Wohnung aufhalte, zu denen er in einem besonderen Vertrauensverhältnis stehe. In einem solchen Fall sei die Wohnraumüberwachung ausnahmsweise nur zulässig, wenn konkrete Anhaltspunkte vorlägen, dass die zu erwartenden Gespräche oder Handlungen einen unmittelbaren Bezug zu einer dringenden Gefahr für die öffentliche Sicherheit aufweisen würden. Eine berechtigterweise begonnene Wohnraumüberwachung müsse aber abgebrochen werden, sobald eine Situation eintrete, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen sei. Zudem sei eine Datenerhebung, die ein durch ein Amts- und Berufsgeheimnis geschütztes Vertrauensverhältnis betreffe, beispielsweise zu einem Geistlichen oder Rechtsanwalt, bereits von Gesetzes wegen ausnahmslos unzulässig. Hingegen gestatte das Gesetz unter engen Voraussetzungen zulässigerweise eine automatisierte Speicherung des Inhalts abgehörter Gespräche. Dies könne etwa erforderlich sein, wenn Gespräche in einer Fremdsprache oder von mehreren Teilnehmern geführt würden.

Die Regelung des § 29 POG wahre auch den Grundsatz der Verhältnismäßigkeit. Die Maßnahme diene dem verfassungsrechtlich legitimen Zweck der Bekämpfung der organisierten Kriminalität und der Gewährleistung eines wirkungsvollen Schutzes der Bevölkerung vor terroristischen Anschlägen. Ihre Eignung zur Erreichung dieses Ziels werde nicht dadurch in Frage gestellt, dass bisher nur eine geringe Zahl von Wohnraumüberwachungen durchgeführt worden sei. Dies beruhe auf dem mit der Maßnahme verbundenen hohen Aufwand und auf der polizeilichen Zurückhaltung beim Einsatz dieses der Gefahrenabwehr dienenden Instruments. Die restriktive Praxis stärke das Vertrauen der Allgemeinheit in eine grundrechtsschonende Überwachungspraxis. Eine weniger grundrechtsbeeinträchtigende Alternative, die der Gefahrenabwehr gleich wirksam diene, sei nicht ersichtlich.

Schließlich sei auch die Überwachung des Wohnraums von so genannten Kontakt- und Begleitpersonen verfassungsrechtlich nicht zu beanstanden, d.h. von Personen, die mit einer anderen, der Begehung zukünftiger Straftaten verdächtigen Person in Verbindung stehen. Eine solche Maßnahme setze als unerlässliche Voraussetzung zum einen das Vorliegen einer dringenden Gefahr für ein hochrangiges Rechtsgut voraus. Zum anderen müsse die Maßnahme zusätzlich der Verhinderung von im Gesetz genannten besonders schweren Straftaten dienen, die ausnahmslos mit einer Höchststrafe von mehr als fünf Jahren bedroht seien.

5.2.2 Evaluation des § 29 POG

Nach § 100 POG ist die Landesregierung verpflichtet, den Landtag bis zum 9.3.2009 über die Wirksamkeit verschiedener im Jahr 2005 neu eingeführter polizeilicher Befugnisse zu unterrichten, insbesondere auch über die akustische und optische Wohnraumüberwachung gem. § 29 POG; diese Maßnahmen unterliegen zudem einer jährlichen Berichtspflicht an den Landtag gem. § 29 Abs. 12 POG.

In den Jahren 2004/2005 wurde nur eine Maßnahme gem. § 29 POG durchgeführt; für das Jahr 2006 erfolgte keine derartige Maßnahme (Bericht über den Einsatz technischer Mittel nach §§ 29, 31 POG für das Jahr 2006, LT-Drs. 15/1502 v. 13. 09. 2007). Damit bestätigt sich die Einschätzung, die der VGH zur Häufigkeit des praktischen Einsatzes dieser Maßnahme formuliert hat (s.o. Tz. 5.2.1).

5.3 Örtliche Feststellungen bei Polizeidienststellen

Ein Großteil der im Berichtszeitraum geprüften polizeilichen Datenverarbeitungen stand im Zusammenhang mit der „Einsatzlage Fußballweltmeisterschaft". Daneben prägten Diskussionen um neue EDV-Anwendungen in der Polizei wie POLADIS-Zentral, KRISTAL und nicht zuletzt die Antiterrordatei die im Berichtszeitraum geführten Beratungs- bzw. Informationsgespräche mit der Zentralstelle für Polizeitechnik, der Projektgruppe POLADIS, dem LKA und dem ISM. Neben häufigen Informationsbesuchen im Ministerium, dem LKA und der Zentralstelle für Polizeitechnik, insbes. der Projektgruppe POLADIS, fanden in den fünf Präsidialbereichen bei neun stichprobenartig ausgewählten Polizeibehörden Kontrollen vor Ort statt. Es war nicht selten, dass als Ergebnis der örtlichen Feststellungen Verbesserungsvorschläge formuliert wurden, deren Umsetzung regelmäßig vom ISM veranlasst wurde. In Einzelfällen war auch anzuregen, Datenspeicherungen in den kriminalpolizeilichen Akten und in der diese erschließenden Datei zu löschen. Auch insoweit wurde regelmäßig Einvernehmen mit allen Beteiligten erzielt.

5.3.1 Speicherung personengebundener Hinweise (PHW) in POLIS/INPOL

Um sich ein Bild von der Datenverarbeitung im Zusammenhang mit Unterlagen und Akten aus den Bereichen der politisch motivierten Kriminalität zu machen, hatte der LfD im Zuständigkeitsbereich dreier Polizeipräsidien jeweils Stichproben kriminalpolizeilicher Akten (KpS) ausgewählt, um herauszufinden, ob in allen geprüften Fällen die Vergabe des PHW angemessen und damit zulässig war, die Speicherfristen der jeweiligen PHW von maximal fünf Jahren eingehalten wurden und in der KpS ausreichende Anhaltspunkte für die Vergabe des personengebundenen Hinweises dokumentiert waren. Als Fazit aus der Prüfung empfahl der LfD, ggf. durch eine Überwachungsliste und eine präzisere Dokumentation von Anlässen, Ereigniszeiten und Prüfungsergebnissen im Zusammenhang mit dem Vorliegen eines Restverdachts die maximale Ausschreibungsdauer von fünf Jahren für die entsprechenden PHW sicherzustellen. Außerdem regte der LfD an, zur Beurteilung der Frage, ob die Voraussetzungen von Tatbeständen wie beispielsweise der Volksverhetzung vom Tatverdächtigen erfüllt wurden, das Gerichtsurteil bei der Staatsanwaltschaft anzufordern und in die KpS aufzunehmen. Die betroffenen Polizeidienststellen sagten zu, künftig entsprechend zu verfahren.

5.3.2 Die Dokumentation von erkennungsdienstlichen Behandlungen in den kriminalpolizeilichen Akten

Es fehlten bei einer Polizeidienststelle verfahrenssichernde Maßnahmen zur Dokumentation der rechtlichen Grundlagen erkennungsdienstlicher Behandlungen in den polizeilichen Akten (den KpS). Die Empfehlung des LfD, die Vorladung bzw. die Anordnung erkennungsdienstlicher Behandlungen, die Unterschrift des erkennungsdienstlich Behandelten unter den Belehrungstext sowie die Belehrung über das Widerspruchsrecht und die Angabe der Rechtsgrundlage der konkreten erkennungsdienstlichen Behandlung in der KpS zu dokumentieren, wurde vom betroffenen Polizeipräsidium umgehend befolgt. Weitere Prüfungen in anderen Landesteilen zu diesem Thema sollen erfolgen, um zu erkennen, ob insoweit auch in anderen Präsidialbereichen Defizite bestehen.

5.3.3 Arztdaten in polizeilichen Ermittlungsverfahren – Medico-Datei

Zur Bekämpfung des durch Ärzte gegenüber der Kassenärztlichen Vereinigung sowie privaten und gesetzlichen Krankenkassen begangenen Abrechnungsbetrugs nutzt die Polizei das Datenbanksystem „Medico", in das alle Informationen einfließen, die sich aus den im Rahmen der Durchsuchung von Arztpraxen beschlagnahmten Patientenakten ergeben. Die Bearbeitung dieser speziellen Form der Wirtschaftskriminalität erfordert besondere Sachkenntnisse. Deshalb wurde die Bearbeitung von Ärzteverfahren Sonderarbeitsgruppen übertragen. Da in diesem Zusammenhang besonders schützenswerte Gesundheitsdaten verarbeitet werden, waren bei Einführung des Datenbanksystems seitens des LfD besondere Anforderungen an die Datensicherheit definiert worden, deren Umsetzung bei einer seit 1998 arbeitenden Arbeitsgruppe geprüft wurde. Schwerpunkte

waren dabei die Prüfung der Zugriffsrechte auf die jeweils benutzten Laufwerke sowie interne Benutzerberechtigungen, die Anbindung des Medico-Servers an das Polizeinetz und die Löschungsmodalitäten abgeschlossener Ermittlungsverfahren. Dabei wurde festgestellt, dass nicht erforderliche Zugriffsberechtigungen existierten, dass eine Ablage der Daten auf dem Server nicht ausreichend verschlüsselt erfolgte und dass die Löschungsmodalitäten bei Verfahren, bei denen das Urteil Rechtskraft erlangt hatte, verbesserungsfähig waren. Im Gegensatz zum LfD sah das ISM in der Verschlüsselung der Medico-Datenbank nur eine ergänzende Option, die für die Ausnahmefälle in Betracht kommt, bei denen der Medico-Server an das VPN-POL angeschlossen ist. Soweit der Medico-Server ohne VPN-POL Anbindung betrieben wird, ist nach Auffassung des ISM eine Verschlüsselung nicht zwingend erforderlich. Die anderen festgestellten datenschutzrechtlichen Defizite wurden zeitnah von der Dienststelle behoben.

5.3.4 Dokumentation des Verfahrensausgangs in polizeilichen Akten (MiStra-Rückläufe)

Gegenstand einer Prüfung waren Verkehrsunfallstraftaten, deren Verfolgung eingestellt oder bei denen die Betroffenen freigesprochen worden waren. Der Verfahrensausgang wird dann regelmäßig von der Polizei in POLADIS.net erfasst. Dies erfolgte zufriedenstellend. Die entsprechende staatsanwaltliche Benachrichtigung (genannt „MiStra“) wird danach dem Sachbearbeiter zugeleitet, der sie vernichtet. Hier empfahl der LfD, nicht nur die MiStra in der Originalakte bei der Staatsanwaltschaft, sondern eine Kopie auch bei der sachbearbeitenden Polizeidienststelle für die Dauer der Datenspeicherung vorzuhalten.

5.4 Die Antiterrordatei

5.4.1 Allgemeines

Mit dem Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22.12.2006, BGBl. I S. 3409, hat der Bundestag mit Zustimmung des Bundesrats eine neue Verbunddatei auf der Ebene des Bundes geschaffen, in der Daten über terrorverdächtige „Gefährder“ für alle Verbundteilnehmer abrufbar gespeichert werden sollen. Das wesentlich Neue an der Antiterrordatei ist die gemeinsame Urheberschaft von Polizei und Verfassungsschutz sowie der gemeinsame Zugriff dieser Behörden auf den gesamten Datenbestand, dessen Inhalt allerdings – wie bei den herkömmlichen polizeilichen Verbunddateien – von der Dienststelle verantwortet wird, die den jeweiligen Datensatz eingestellt hat.

5.4.2 Verfassungsrechtliche Fragen

Umstritten ist, ob diese Durchbrechung des sog. Trennungsgebotes verfassungsrechtlich zulässig ist. Außerdem wird in Frage gestellt, ob die gesetzlichen Kriterien für die Aufnahme von Personen in diese Datei klar genug sind. Es wird befürchtet, dass zu viele und ungeeignete Daten zu unverhältnismäßigen Belastungen letztlich unschuldiger Personen führen (vor allem auch bei den „Kontaktpersonen“). Diese Bedenken hat der LfD mit Blick auf die im Land zu erwartende zurückhaltende Praxis nicht für so gravierend gehalten, dass sie zum Verdikt der Verfassungswidrigkeit des Gesetzes führen müssten. Zudem ist anzuerkennen, dass der Gesetzgeber Vorkehrungen gegen eine unverhältnismäßige Nutzung getroffen hat: nur vergleichsweise wenige Personen innerhalb der angeschlossenen Organisationen haben Zugriffsrechte; die gesetzlich vorgegebene organisatorische Schranke vor dem Zugriff auf die erweiterten Grunddaten (Genehmigungserfordernis der einspeichernden Stelle) dient dem Datenschutz. Umfangreiche Protokollierungen ermöglichen nachträgliche Kontrollen. Die getroffenen Maßnahmen des technisch-organisatorischen Datenschutzes sind auch aus dem Eigeninteresse der beteiligten Stellen am Schutz vor Ausforschung kaum zu übertreffen.

Eine anhängige Verfassungsbeschwerde wird dem Bundesverfassungsgericht Gelegenheit geben, die verfassungsrechtlichen Fragen abschließend zu beurteilen.

5.4.3 Erkenntnisse zur praktischen Nutzung

Zur Vorbereitung örtlicher Feststellungen und zur Ergänzung seiner Stellungnahme gegenüber dem Bundesverfassungsgericht im o.g. Verfassungsbeschwerdeverfahren hat sich der LfD darum bemüht, Erkenntnisse über die praktische Nutzung der Antiterrordatei in Rheinland-Pfalz zu gewinnen. Seine detaillierten Fragen dazu wurden vom ISM (der Polizeiabteilung und dem Verfassungsschutz) bereitwillig beantwortet. Die entsprechenden Angaben wurden aber als Verschlusssache (Nur für den Dienstgebrauch) klassifiziert, so dass damit die Übermittlung an das Bundesverfassungsgericht ausgeschlossen wurde. Dies ist aus der Sicht des LfD sehr zu bedauern, da ein Einblick in die tatsächliche Nutzung der Datei dem Verfassungsgericht sicherlich eine bessere Einschätzung der hier erfolgenden Eingriffe in die Grundrechte der Bürger ermöglichen würde. Veröffentlichungsfähig

ist aus der Sicht der zuständigen Behörden allein die Angabe über die Gesamtzahl der erfassten Datensätze. Diese betrage (Stand 13.9.2007) insgesamt 15.710 Personen, davon 791 Doubletten.

5.4.4 Protokollierung und Protokolldatenauswertung

Maßstab der Anforderungen an die Protokollierung ist § 9 Abs. 1 Satz 1 ATDG. Dieser sieht für (lesende) Zugriffe vor, dass für Zwecke der Datenschutzkontrolle Zeitpunkt, verantwortliche Behörde, Zugriffszweck und die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, zu erfassen sind. Es ist vorgesehen, dass das BKA zentral die Zugriffsprotokollierungen auf die Antiterrordatei durchführt. Nach den dem LfD gegenüber gemachten Aussagen beschränken sich die derzeitigen Auswertungsmöglichkeiten auf die Kriterien „Anfrager", „Zeitraum" und „getroffene Person" sowie deren UND-Kombination. Vor dem Hintergrund der o.g. Regelung griffe dies zu kurz. Nach Aussage des BKA bestehe bei Bedarf zwar die Möglichkeit, auch speziellere Auswertungen durchzuführen, der Umfang der über das Auswertewerkzeug bereitgestellten Standardabfragen solle jedoch beschränkt sein. Die Möglichkeit von Sonderauswertungen, etwa weil sich im Rahmen einer Kontrolle weitergehende Fragen ergeben, ist für eine effektive Datenschutzkontrolle aber unverzichtbar. In jedem Fall sollten **Standardauswertungen** bereits die in § 9 Abs. 1 ATDG genannten Kriterien abdecken.

Dies bedeutet für das Merkmal:

- „für den Zugriff verantwortliche Behörde"
  Um ohne großen Aufwand eine Aussage darüber zu erhalten, von wem eine Abfrage vorgenommen wurde, sollte es sich daher bei zu protokollierenden Information um die Benutzerkennung handeln, wie sie nach dem Rollen- und Berechtigungskonzept des BKA von den Ländern jeweils vergeben wurde. Eine Auskunft wie z.B. „Anitterrordateinutzer aus Rheinland-Pfalz" wäre zu allgemein.
- „Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen"
  Das Auswertewerkzeug sollte Suchfelder entsprechend den Abfragemöglichkeiten (Person, Fahrzeug, E-Mail, Telefon etc.) und Zusatzkriterien (Grund der Anfrage, Suchoption mit/ohne verdecktem Bestand, Dringlichkeit und Suchbereich) der Antiterrordatei vorsehen, um nachvollziehen zu können, wann, von wem und mit welchen Suchkriterien eine Abfrage vorgenommen wurde.

Für die erforderlichen **Sonderauswertungsmöglichkeiten** gilt: Die bislang vorgesehenen Auswertungsmöglichkeiten decken lediglich Fragestellungen ab, die sich an einem konkreten Ereignis festmachen lassen (z.B. Wurde und ggf. wann und von wem auf die Person XY abgefragt?). Fragen, die darauf abzielen, ein ungewöhnliches oder auffälliges Abfrageverhalten zu erkennen, können daraus nicht beantwortet werden.

Aufgrund vorhandener Erkenntnisse über die Nutzung anderer Großverfahren sollten sich im Rahmen der Datenschutzkontrolle der Antiterrordateiprotokolle aber z.B. auch folgende Fragen beantworten lassen (jeweils bezogen auf abfragende Stellen aus dem Zuständigkeitsbereich des jeweiligen Datenschutzbeauftragten):

- Welche Abfragen sind ohne Namen lediglich mit der Angabe des Wohnorts (Kfz-Kennzeichen, Telefonnummer, Mailadresse o.ä.) erfolgt?
- Welche Abfragegründe wurden von einer bestimmten Benutzerkennung angegeben?
- Welche Abfragen haben zu Rückweisungen wegen unzureichender Berechtigungen geführt?
- Welche Abfragen haben zu Ersuchen zur Ansicht erweiterter Grunddaten eines Objekts geführt?
- Bei welchen Abfragen wurde die „Eilfall-Freischaltung" in Anspruch genommen; welche Begründungen wurden hierbei angegeben?

Daneben sind statistische Auswertungen von Bedeutung, wie

- Anzahl der Abfragen für eine bestimmte Benutzerkennung
- Anzahl der Abfragen eines Landes/des Bundes insgesamt
- Anzahl der Abfragen auf die offenen Datensätze eines Landes/des Bundes
- Anzahl der Abfragen auf die verdeckten Datensätze eines Landes/des Bundes
- Anzahl der von einem Land/dem Bund eingestellten offenen Datensätze
- Anzahl der von einem Land/dem Bund eingestellten verdeckten Datensätze

Vorzugsweise sollten die dargestellten Abfragen über das vom BKA vorgesehene Auswerteprogramm vorgenommen werden können. Akzeptabel erscheint jedoch auch, wenn dies, im Zeitrahmen einer Kontrolle, über separate Abfrageskripts erfolgt. Neben den in § 9 Abs. 1 ATDG angesprochenen lesenden Zugriffen gelten die dargestellten Anforderungen entsprechend § 9 Abs. 2 ATDG i.V.m. Nr. 5 der zugehörigen Anlage sinngemäß auch für schreibende Zugriffe (erstmalige Speicherung, Änderung

und Löschung). Die Funktionalität der Antiterrordatei wird nach Aussage des BKA im Rahmen kommender Releases erweitert. So soll künftig die Möglichkeit bestehen, nach Beziehungen zwischen Personen zu recherchieren bzw. nach „Verfahren“ und diesen zugeordneten Personen und deren erweiterten Grunddaten. Soweit derartige Funktionserweiterungen vorgenommen werden, müssen grundsätzlich auch die Möglichkeiten der Protokollauswertung nachgeführt werden.

Der LfD hat diese Anforderungen gegenüber dem ISM und – über den BfDI – auch an das BKA gerichtet. Derzeit ist darüber noch nicht abschließend entschieden worden. Der LfD wird sich – gemeinsam mit dem BfDI – weiter um eine datenschutzgerechte Ausgestaltung der Protokollierungen im Rahmen der Antiterrordatei bemühen; nur bei einem Erfolg dieser Bemühungen können effiziente Datenschutzkontrollmaßnahmen in Bezug auf die Nutzung der Antiterrordatei erfolgen.

5.5 Die Einrichtung von Sexualstraftäterdateien

Im Berichtszeitraum wurde von verschiedener Seite die Einrichtung von Sexualstraftäterdateien im Internet zum Abruf für Jedermann gefordert. Dem ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder entschieden entgegen getreten. Sie hält solche Pläne für verfassungswidrig. In einer Entschließung (vgl. Anlage 23) führt sie u.a. aus, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssten. Dies schließe jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zustehe.

Als Alternative wird derzeit erörtert, über eine Sexualstraftäterdatei, die nur den zuständigen Stellen zugänglich sein soll, Rückfällen verurteilter Sexualstraftäter wirksamer entgegen zu wirken.

Bayern hat ein entsprechendes Modell bereits eingeführt: die Sexualstraftäterdatei „HEADS“ (Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter) wurde zum 1.10.2006 beim Polizeipräsidium München eingerichtet. Mit ihr soll der Informationsfluss zwischen Justiz, Polizei und Maßregelvollzug über die Daten aus der Haft entlassener gefährlicher Sexualstraftäter verbessert werden. Die Staatsanwaltschaft informiert die „Zentralstelle HEADS“ bei der Entlassung besonders rückfallgefährdeter Sexualstraftäter und übermittelt alle „für eine polizeiliche Bewertung notwendigen Unterlagen“. In HEADS werden die Daten erfasst und den zuständigen Polizeidienststellen zur Verfügung gestellt, die dann Überwachungsmaßnahmen festlegen und mit Führungsaufsicht, Bewährungshilfe, Polizei, Kreisverwaltungsreferaten sowie Jugendämtern koordinieren sollen. Der Datenschutz werde dadurch gewahrt, dass die Daten nur von den Experten einer Polizeizentralstelle abgerufen werden könnten. Der bayerische LfD hat diesem Verfahren – allerdings nur vorläufig – zugestimmt.

Auch in unserem Land wird erörtert, ob dieses Modell übertragbar ist. Aus Sicht des Datenschutzes ist die Frage zu klären, ob wirklich nur die zuständigen Stellen im erforderlichen Umfang entsprechende Daten erhalten würden. Grundsätzliche Bedenken stehen einer solchen Verfahrensweise aber nicht entgegen. Der Landtag hat sich in verschiedenen Ausschüssen dieser Problematik angenommen. Der LfD hat dabei insbesondere die bayerische Praxis erläutert.

5.6 Die Nutzung privater Videoüberwachungsanlagen durch die Polizei

Die Polizei prüft derzeit auf der Basis eines Beschlusses der Innenministerkonferenz, ob sie die Videoüberwachungsanlagen nichtöffentlicher Stellen landesweit erfasst und einen sogenannten „Videoatlas“ erstellt. In Baden-Württemberg wurde eine entsprechende Aktion bereits durchgeführt. Sie hat in den Medien bundesweit eine erhebliche Resonanz gefunden, zumal der Innenminister ankündigte, die Polizei wolle sich bei Bedarf auf die privaten Videoüberwachungsanlagen „aufschalten“.

Derzeit ist noch unklar, ob in Rheinland-Pfalz entsprechend verfahren wird. Aus der Sicht des LfD müsste vorab jedenfalls das rheinland-pfälzische Polizeigesetz novelliert werden, in dem – wenn diese Vorstellungen der Innenminister realisiert werden sollten – die Rechtsgrundlagen für eine derartige Inpflichtnahme Privater zu schaffen wären. Dem müssten in jedem Fall aber intensive Erörterungen zur Klärung der datenschutzrechtlichen Fragen vorausgehen, ob das Vorhaben insgesamt verhältnismäßig und geeignet ist sowie, unter welchen Voraussetzungen ggf. eine Aufschaltung auf private Videoüberwachungsanlagen erfolgen darf und welche technisch-organisatorischen Datenschutzmaßnahmen angemessen sind.

5.7 Die Zentralisierung des polizeilichen Vorgangsbearbeitungssystems POLADIS

Das polizeiliche anwenderorientierte Daten- und Informationssystem (POLADIS) soll zunächst und in erster Linie der Vorgangsbearbeitung und -verwaltung dienen. Dementsprechend ist es dezentral so aufgebaut, dass grundsätzlich die lokalen

Polizeidienststellen dieses System auf eigenen Servern vorhalten. Schon deshalb gibt es keine Vernetzung der Daten; ein überregionaler Datenzugriff ist nahezu unmöglich.

Nunmehr wird aus ökonomischen und technischen Gründen (der besseren Verwaltung und leichteren Betreuung des Systems wegen) eine zentrale Datenverarbeitung für dieses Verfahren geplant. Mit der Zentralisierung von Poladis.net sollen die bisher dezentral auf den Polizeidienststellen gespeicherten Datenbestände in eine zentrale Datenbank überführt und ausschließlich dort als Gesamtdatenbestand vorgehalten werden. Dieses Verfahren soll künftig den Polizeibeamten landesweite Recherchen eröffnen. Damit geht ein grundlegender Wandel des Systems einher: Es wird künftig in einem erheblichen Maß als landesweites Informationssystem der Polizei auch zur Unterstützung polizeilicher Ermittlungstätigkeiten genutzt werden. Dies ist deshalb aus datenschutzrechtlicher Sicht problematisch, weil die Kriterien für die Datenspeicherungen in diesem System einen ganz anderen Hintergrund haben: Eine Information darüber, ob ein Beschuldigter im weiteren Verfahren entlastet oder sogar freigesprochen wurde, ob ein Verdacht im Laufe der Ermittlungen erhärtet wurde oder ob er entfallen ist, ist diesem System grundsätzlich nicht zu entnehmen. Darauf ist es nicht ausgerichtet. Die Arbeiten der hierzu vom ISM beim Landeskriminalamt eingesetzten Arbeitsgruppe zur Erstellung eines dezidierten Rollen- und Berechtigungskonzeptes sind noch nicht abgeschlossen. Fest steht, dass für die überwiegende Anzahl der rheinland-pfälzischen Polizeibeamten lediglich die Funktion „landesweite Vorgangssuche“ bereitgestellt werden wird. Diese Funktion soll nur einen Teilausschnitt von Vorgangsdaten im Lesezugriff zur Verfügung stellen und damit im Wesentlichen die Rolle eines „landesweiten Tagebuches“ erfüllen. Das ISM geht davon aus, dass bei der Umsetzung dieser Funktion auch der jeweilige Vorgangsstatus (Verantwortlicher bzw. Nichtverantwortlicher) eine entsprechende Berücksichtigung finden wird. Die weiteren neuen Recherchefunktionen (insbesondere „Volltextsuche“ und „Report“) werden dagegen nur ausgewählten Funktionsbereichen mit speziellem Auswerteauftrag zur Verfügung stehen.

Wenn die Funktion als polizeiliches Informationssystem betont werden wird, werden aus der Sicht des LfD Vorkehrungen erforderlich, damit solche Informationen, die für eine Bewertung der gespeicherten Daten unerlässlich sind, auch zur Verfügung gestellt werden. Mit der Zentralisierung sind weitere datenschutzrechtliche Anforderungen verbunden, wie z.B. Protokollierungsmechanismen, Zugriffsmöglichkeiten auf Protokolldaten zu Datenschutzkontrollzwecken auch vor Ort, Berechtigungskonzepte und Schranken, die eine mißbräuchliche Nutzung verhindern. Diese Fragen werden derzeit mit dem ISM abgestimmt.

5.8 Das kriminalpolizeiliche Recherche- und Auswertesystem (KRISTAL)

Das Kriminalpolizeiliche Recherche und Informationssystem – Täterorientierte Auswertung, Analyse und Lagedarstellung – „KRISTAL“ unterstützt die Ermittlungen der Polizei im Rahmen vorbeugender Verbrechensbekämpfung und bei der Durchführung von Ermittlungsverfahren.

Derzeit sind in KRISTAL zwei Anwendungsbereiche realisiert:

- Organisierte Kriminalität (OK) und
- Politisch motivierte Kriminalität (PMK).

Daneben wurden definierte Schnittstellen neu geschaffen, die einen Import von TKÜ- und Anschlussinhaberdaten in die einzelnen KRISTAL-Verfahren ermöglichen. Geplant sind darüber hinaus die Anwendungsbereiche „Menschenhandel“ und „Kapitaldelikte“. Die zunächst pilotierten Bereiche OK und PMK sind seit Ende 2006 im Wirkbetrieb.

Aus Datenschutzsicht sind diese neuen Verfahren aus folgenden Gründen bedeutsam:

Sie erlauben die Verknüpfung und das rasche Auffinden der verschiedensten Informationen; Texte, Bilder und sogar Tondokumente sind integriert; komplexe Sachverhalte können grafisch dargestellt werden.

Die Dateien sind landesweit zwischen den jeweiligen Fachkommissariaten verknüpft. KRISTAL verfügt über einen dateiübergreifenden automatisierten Datenabgleich mit der Konsequenz, dass automatisiert eine Warnmeldung erzeugt wird, wenn eine Personalie erfasst wird, zu der bereits in einer anderen Datei Informationen vorhanden sind. Zwischen den Dateien OK und PMK bestehen allerdings keine Verbindungen.

Der Empfehlung des LfD, für diese erweiterte Anwendung die Zugriffsberechtigungen in der Generalerrichtungsanordnung für KRISTAL entsprechend zu regeln, wurde entsprochen. Darüber hinaus hatte der LfD die Handhabung der Aussonderungsprüffristen problematisiert, weil systemseitig lediglich ein Button „Prüfe in 28 Tagen“, jedoch keine automatisierte Unterstützung angeboten wird. Die an sich wünschenswerte automatisierte Löschung konnte zunächst nicht realisiert werden. Ersatzweise hat der LfD bei Fristüberschreitung zumindest die Fertigung von automatisierten „Warnlisten“ empfohlen, da eine bloß manuelle Kontrolle ohne technische Unterstützung durch Sachbearbeiter oder die Fachaufsicht als

datenschutzrechtlich nicht ausreichend anzusehen ist. Das ISM hält dagegen die derzeitige Verfahrenspraxis (intensive Fachaufsicht durch das Landeskriminalamt) und Prüfpflicht durch den jeweiligen Sachbearbeiter für datenschutzrechtlich ausreichend.

5.9 INPOL-neu – datenschutzrechtliche Begleitung

Das BKA ist nach dem BKAG Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern. Es ist damit technisch verantwortlich für die in das polizeiliche Informationssystem einzubeziehenden Dateien. Teilnehmer am polizeilichen Informationssystem mit dem Recht, Daten im automatisierten Verfahren einzugeben und abzurufen, sind außer dem BKA und den Landeskriminalämtern sonstige Polizeibehörden der Länder, die Bundespolizei sowie Behörden der Zollverwaltung und das Zollkriminalamt (§ 11 BKAG). Dieser polizeiliche Informationsverbund wird mit dem Begriff „INPOL“ bezeichnet. Es handelt sich dabei um einen inzwischen nur noch schwer überschaubaren Komplex von Dateien und Anwendungen. Sowohl die technischen Grundlagen wie die Funktionalitäten des Systems sind ständigen Änderungen unterworfen. Es ist ein selbstverständliches Anliegen der Datenschutzbeauftragten, in diese Entwicklung einbezogen zu werden. Der BfDI kann diese Aufgabe schon deshalb nicht allein übernehmen, weil in INPOL Bund und Länder untrennbar zusammenwirken müssen; Gleiches gilt dementsprechend auch für die Kontrollbehörden.

Um die ständige Begleitung der INPOL-Entwicklung zu ermöglichen, haben die Datenschutzbeauftragten von Bund und Ländern eine Arbeitsgruppe eingerichtet, in der neben dem Bund die Länder Schleswig-Holstein, Hessen und Rheinland-Pfalz mitwirken. Die Bemühungen der Arbeitsgruppe um einen stetigen Informationsfluss und auch um die Möglichkeit, Datenschutzgesichtspunkte frühzeitig in die Entwicklung einzubringen, sind als dauernde Aufgabe anzusehen. Es ist eine deutliche Bereitschaft des BKA festzustellen, diese Aufgabe zu unterstützen.

5.10 ED-Daten aus Rheinland-Pfalz beim Bundeskriminalamt

Daten von erkennungsdienstlich behandelten Personen werden zentral beim BKA gespeichert. Verantwortliche Stellen, auch im Hinblick auf die Datenlöschung, bleiben aber diejenigen Behörden, die die Daten erhoben und in die Datei eingestellt haben. Dies sind in der größten Zahl der Fälle Landespolizeibehörden.

Beim BKA sind die ED-Daten grundsätzlich nach festgelegten Fristen auf ihre Löschungsmöglichkeit hin zu überprüfen. Eine vorzeitige Löschung muss erfolgen, wenn die verantwortliche Stelle, die die Daten eingespeichert hat – im Regelfall also das jeweilige LKA – eine vorzeitige Löschung der Daten verfügt, etwa aufgrund eines gerichtlichen Freispruchs oder einer Einstellung des Verfahrens wegen fehlenden Tatverdachts, wenn aus polizeilicher Sicht kein Restverdacht fortbesteht und keine Wiederholungsgefahr angenommen werden muss. In der Praxis übernimmt das BKA in diesen Fällen aber grundsätzlich den Besitz an den ED-Daten des Landes und speichert die Daten bis zum Ablauf einer zehnjährigen Speicherfrist, obwohl die näheren Umstände der Datenerhebung dem BKA unbekannt sind und obwohl die bei der zuständigen Polizeidienststelle des Landes bestehende Kriminalakte gelöscht wurde. Die Kenntnis der sich aus der Kriminalakte ergebenden Gesamtumstände sind aber erforderlich, um die gesetzlich geforderte sog. Negativprognose erstellen zu können. Diese Negativprognose ist Voraussetzung für die weitere Speicherung und kann nur abgegeben werden, wenn etwa wegen eines fortbestehenden Verdachts der Tatbegehung und der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass künftig weitere Verfahren gegen ihn zu führen sind. Das BKA kennt in der Regel nur den Tag der ED-Maßnahme, das Delikt und die zuständige Polizeidienststelle. Die Tatsache, wie das Verfahren zwischenzeitlich beendet worden ist, kann nicht hinzugespeichert werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten dieses Verfahren für nicht hinnehmbar. Wenn die Daten durch die Landespolizei gelöscht werden, muss das BKA dem folgen, wenn es nicht selbst weitergehende Erkenntnisse über den Betroffenen hat. Die Datenschutzbeauftragten unter Einschluss des BfDI bemühen sich weiter um eine Lösung dieses Problems.

5.11 Funkzellenabfragen

Ziel der Funkzellenabfrage ist die Feststellung, welche Mobilfunktelefongeräte in einer oder mehreren benachbarten Funkzellen zu einem bestimmten Zeitpunkt oder in einem bestimmten Zeitraum aktiv geschaltet waren. In Deutschland gibt es vier Mobilfunknetze. Jedes Mobilfunknetz ist geografisch in viele aneinandergrenzende Gebiete unterteilt – die so genannten Funkzellen. Man spricht daher auch vom zellularen Aufbau der Netze. Die Aufteilung in Funkzellen von begrenzter Größe ermöglicht es, die beschränkte Anzahl verfügbarer Funkkanäle optimal zu nutzen, denn die Menge an verfügbaren Funkfrequenzen ist beim Mobilfunk stark begrenzt. Auf dem Weg der Funkzellenabfrage kann mit einer gewissen Wahrscheinlichkeit festgestellt werden, welche Personen sich zu einem für die Straftatenaufklärung als relevant angesehenen Zeitpunkt in einem bestimmten Gebiet aufgehalten haben. Die Strafverfolgungsbehörden, in erster Linie die Polizei, können solche

„Funkzellenabfragen“ gem. §§ 100 g, 100 h Abs. 1 Satz 2 StPO durchführen. Zu diesem Zweck müssen alle vier deutschen Netzbetreiber (T-Mobile, Vodafone, E-Plus und O_2) unter Angabe der genauen Funkzelle und des Zeitraums, der untersucht werden soll, um Auskunft ersucht werden.

Der LfD hat hierzu in zwei Präsidialbereichen des Landes eigene Feststellungen getroffen. Funkzellenüberwachungen sind aus polizeilicher Sicht nicht leicht durchzuführen.

- Sie verursachen einen hohen Ermittlungsaufwand – durchschnittlich kann je nach Art der Funkzelle pro Überwachungsmaßnahme von einem Datenvolumen zwischen 900 bis 30.000 aufgelisteten Einzelverbindungen ausgegangen werden.
- Bei der Durchführung müssen hohe rechtliche Anforderungen erfüllt sein – es muss ein Fall schwerer Kriminalität mit hohem Unwertgehalt der Straftat vorliegen, §§ 100 g, 100 h StPO, und alle anderen erfolgversprechenden Ermittlungsansätze müssen ausgeschöpft sein.
- Es sind nur relativ wenige ausgebildete Mitarbeiter vorhanden, die in der Lage sind, die erforderliche komplexe Datenauswertung vorzunehmen.

Dennoch kann gesagt werden, dass die Funkzellenüberwachung für die Aufklärung von Kapitalverbrechen als Standardmaßnahme anzusehen ist. Das datenschutzrechtliche Problem besteht bei solchen Maßnahmen vor allem darin, dass grundsätzlich eine große Zahl von Personen festgestellt wird und dass häufig nicht feststeht, ob auch nur eine der damit erfassten Personen als Beschuldigter anzusehen ist. Darüber hinaus ist rechtlich problematisch, dass sich diese Maßnahme faktisch nicht nur gegen Beschuldigte oder auch nur möglicherweise beschuldigte Personen richtet, sondern schwerpunktmäßig und vor allem gegen unbeteiligte Dritte. Dies ist besonders dann der Fall, wenn nicht einmal feststeht, ob der mutmaßliche Täter überhaupt ein Mobilfunktelefongerät mit sich geführt hat.

Insbesondere weil auch die lange Speicherdauer der Daten Unbeteiligter nicht frei von datenschutzrechtlichen Bedenken ist, wurde mit dem ISM erörtert, einschränkende bzw. klarstellende gesetzliche oder untergesetzliche Regelungen (oder auch „Handlungsempfehlungen“) für den Einsatz dieser Ermittlungsmaßnahme zu schaffen. Diese Bemühungen sind noch nicht abgeschlossen.

5.12 Einzelfälle

5.12.1 Unterrichtung des Dienstherrn eines Beamten oder des Arbeitgebers durch die Polizei über das Fehlverhalten eines Beschäftigten

Ein Postbeamter war mehrfach (insgesamt war von fünf Ereignissen die Rede) nachts oder in den frühen Morgenstunden (außerhalb seiner regulären Dienstzeit) auf Grund von Trunkenheit auf der Straße oder in einer Gaststätte liegend in einer hilflosen Lage angetroffen worden. Dabei hatte er seine Uniform getragen, die ihn für die Öffentlichkeit als Angehörigen der Post AG ausgewiesen hatte. Außerdem hatte er ein Postfahrrad mitgeführt.

In diesem Zusammenhang hat der LfD die Auffassung vertreten, dass es für einen Beamten als Dienstvergehen zu werten sei, wenn er schuldhaft die ihm obliegenden Pflichten verletzt. Auch wenn sich der Alkoholabusus (bisher nur) außerhalb des Dienstes gezeigt hatte, ist dieses Verhalten – gemessen an den Umständen des Einzelfalles – in besonderem Maße geeignet gewesen, Achtung und Vertrauen in einer für das Amt des betroffenen Beamten und in einer für das Ansehen des Beamtentums bedeutsamen Weise zu beeinträchtigen. Als Dienstvergehen ist außerdem die (schuldhafte) Verursachung einer Alkoholabhängigkeit anzusehen, denn der Beamte ist zur Erhaltung seiner Arbeitskraft verpflichtet und hat ggf. die beschränkte oder verlorene Arbeitskraft bestmöglich wieder herzustellen.

Eine entsprechende Informationsübermittlung hat der LfD deshalb nach § 34 Abs. 2 POG für zulässig gehalten, um dem im datenschutzrechtlichen Sinn als öffentliche Stelle anzusehenden Empfänger (der Post AG) die Erfüllung seiner Aufgaben zu ermöglichen.

Davon unterschied sich ein anderer Sachverhalt, der dem LfD von der Polizei vorgetragen wurde: Ein Beschäftigter eines großen Chemieunternehmens im Land war im Straßenverkehr wegen Fahrens unter Alkoholeinfluss auffällig geworden. Die Polizei befürchtete, er könne wegen seiner Verantwortung im Unternehmen Gefahren verursachen, wenn er während der Arbeitszeit Alkohol konsumieren würde. Der LfD hat dazu folgende Auffassung vertreten: Der Arbeitgeber des Betroffenen war ein privates Unternehmen, keine öffentliche Stelle im Sinne des Datenschutzrechts. Der Betroffene war nicht wiederholt auffällig geworden. Der festgestellte Blutalkoholgehalt und das Verhalten des Betroffenen ließen nicht den Schluss auf gewohnheitsmäßigen erheblichen Alkoholmissbrauch während der Arbeitszeit zu. Damit war nicht vom Vorliegen einer konkreten Gefahr

auszugehen, zu deren Abwendung eine Unterrichtung des Arbeitgebers gem. § 34 POG zulässig gewesen wäre. Eine Benachrichtigung des Arbeitgebers kam also nicht in Betracht. Die Polizei teilte diese Auffassung.

5.12.2 Durchsuchung trotz richterlicher Ablehnung des Durchsuchungsbeschlusses

Trotz Vorliegens eines die Hausdurchsuchung ausdrücklich ablehnenden richterlichen Beschlusses hatte die Polizei im Rahmen eines Strafverfahrens die Wohnung eines Beschwerdeführers durchsucht. Die handelnden Polizeibeamten erklärten dies damit, die fragliche Durchsuchung sei Teil eines großen Verfahrens gewesen, in dessen Verlauf viele Durchsuchungsanordnungen richterlich ergangen seien. Sie hätten dabei schlicht übersehen, dass der Richter in einem Fall die Anordnung abgelehnt hätte. Der LfD hat über die Glaubwürdigkeit eines solchen Vorbringens nicht zu urteilen; für ihn ist zunächst die objektiv in solchen Fällen immer gegebene Verantwortung der Stelle maßgeblich, für die die Bediensteten konkret handeln. Weiter ist bedeutsam, welche organisatorischen, verfahrensmäßigen und personalbezogenen Vorkehrungen getroffen werden, um ein entsprechendes datenschutzrechtlich bedeutsames Fehlverhalten zu verhindern. Vorliegend wurde in das Wohnungsgrundrecht, das durch Art. 13 GG geschützt ist, unzulässig eingegriffen. Gleichzeitig wurde auch das Datenschutzgrundrecht verletzt, denn mit dem Eindringen in die Wohnung werden die persönlichen Lebensumstände eines Bürgers, möglicherweise auch Umstände, die zum engsten Kern persönlicher Lebensgestaltung gehören, offenbart.

Auch wenn der Vorfall sich auf einen Einzelfall beschränkte und die in Rede stehende Polizeibehörde Maßnahmen getroffen hat, die auf eine Vermeidung von Wiederholungen abzielen, konnte von einer förmlichen Beanstandung des betroffenen Polizeipräsidiums nicht abgesehen werden, da dieser unzulässige Eingriff als so schwerwiegend anzusehen ist, dass kein Ausnahmetatbestand angenommen werden konnte, der das Absehen von einer Beanstandung erlaubt hätte (gem. § 25 Abs. 2 LDSG).

5.12.3 Übermittlung der Daten eines „Planespotters“ an die amerikanische Militärpolizei

Ein Bürger, dessen Hobby das Fotografieren von Flugzeugen ist (ein sog. „Planespotter“), nutzte die Umgebung eines amerikanischen Militärflugplatzes, um Bilder zu schießen. Die amerikanische Militärpolizei kannte die deutsche Rechtslage, wonach dies im vom Betroffenen eingehaltenen Abstand aus zulässig ist, nicht. Sie wollte die Personalien prüfen und rief nach der Weigerung des Betroffenen die deutsche Polizei zu Hilfe.

Auch die deutschen Beamten verkannten zunächst die Sachlage; sie gingen von dem Verdacht des sicherheitsgefährdenden Abbildens nach § 109 g StGB i.V.m. Art. 7 Abs. 2 Nr. 4 Viertes Strafrechtsänderungsgesetz bzw. einer Ordnungswidrigkeit nach § 5 Abs. 2 i.V.m. § 27 Schutzbereichsgesetz aus und stellten die Identität des Betroffenen fest. Dabei ließen sie es zu, dass die amerikanischen Militärpolizisten die Personalien des Betroffenen durch Einsichtnahme in den Personalausweis zur Kenntnis nahmen und notierten. Das ISM vertritt die Auffassung, dass die Datenübermittlung in diesem Fall nicht unzulässig war, weil die eingesetzten Polizeibeamten nicht in Verkennung der Sachlage gehandelt hatten. Sie hätten nur die Maßnahmen getroffen, die zur Aufklärung des Sachverhaltes (darunter auch die Prüfung bzw. den Ausschluss der Verdachtslage gemäß § 109g StPO) erforderlich gewesen seien. Es habe letztlich nicht sicher geklärt werden können, ob die diesbezüglichen Ermittlungen bei Zulassen der Einsichtnahme bereits abgeschlossen gewesen waren. Der in Rede stehende Straftat- und Ordnungswidrigkeitenverdacht wurde aber bereits unmittelbar vor Ort durch Inaugenscheinnahme der gefertigten Digitalfotos ausgeräumt. Eine Datenübermittlung auf der Grundlage des Art. VII Abs. 6 a NATO-Truppenstatut war also unzulässig. Diese Auffassung wurde vom Innenministerium selbst nach einer entsprechenden Anfrage des LfD vertreten. Das Ministerium folgte der Empfehlung des LfD, die im Umfeld von US-amerikanischen Militärflugplätzen eingesetzten Polizeibeamten darauf hinzuweisen, dass auch eine auf der Grundlage des Art. VII Abs. 6 a NATO-Truppenstatut an sich rechtmäßige Datenübermittlung dann unzulässig ist, wenn der Verdacht einer Straftat (oder Ordnungswidrigkeit) bereits vor Ort ausgeräumt werden kann. Ob dies dem Betroffenen bei seiner nächsten Einreise in die USA helfen wird, bleibt allerdings unklar.

5.12.4 Informelle polizeiliche Hilfe

Ein Polizist beschaffte einem befreundeten Tankstellenbetreiber „aus Gefälligkeit“ inoffiziell die Personalien von Kunden, die seine Tankstelle verließen, ohne zu bezahlen. Die Kraftfahrzeugkennzeichen hatte der Tankwart in seiner Videoüberwachungsanlage gespeichert. Der Beamte erfragte dann telefonisch beim Kraftfahrtbundesamt die Halterdaten. Eine betroffene Kundin, die erklärte, sie habe nur aus Versehen nicht bezahlt, fühlte sich durch dieses Verfahren in ihren Datenschutzrechten insbesondere auch deshalb verletzt, weil die Staatsanwaltschaft das Ermittlungsverfahren zu der von ihr angezeigten Straftat wegen Verletzung des Amtsgeheimnisses durch den Polizisten eingestellt hatte. Sie wandte sich deshalb an den LfD.

Die Staatsanwaltschaft kam in dieser Angelegenheit zu der – aus der Sicht des LfD zutreffenden – Bewertung, dass unter keinem Gesichtspunkt die Tatbestandsvoraussetzungen des Ausspähens von Daten (§ 202 a StGB) erfüllt worden seien und der – aus der Sicht des LfD unzutreffenden – Annahme, dass auch keine Strafbarkeit der Verletzung eines Amts- bzw. Dienstgeheimnisses (§§

203 Abs. 2, 353 b StGB) vorläge. Sie stellte deshalb das Verfahren ein. Der Polizeibeamte hatte sich aber auch nach Auffassung der Staatsanwaltschaft dienstpflichtwidrig verhalten, weil die Halterabfrage nicht dienstlich veranlasst gewesen sei. Dies nahmen die Vorgesetzten des Beamten zum Anlass, sein Verhalten als Dienstvergehen einzustufen, mit ihm sein Fehlverhalten zu erörtern und darauf hin zu wirken, dass von ihm künftig keine personenbezogenen Informationen „inoffiziell" auf dem kurzen Weg erhoben und an Private übermittelt werden. Der LfD hält diese Reaktion insgesamt für angemessen und ausreichend. Er wird sich aber weiter darum bemühen, die Staatsanwaltschaften davon zu überzeugen, dass die Daten des Kraftfahrtbundesamtes in Flensburg keine öffentlich zugänglichen Informationen sind und deshalb unter dem Schutz der Strafbewehrung der §§ 203 Abs. 2 und 353 b StGB stehen.

5.12.5 Zusicherung der Vertraulichkeit von Beschwerden gegen Polizeibeamte im Internet

Im Internetangebot der Polizei wies ein Polizeipräsidium auf seine Beschwerdestelle hin. Bürger wurden darüber unterrichtet, dass sie sich im Bedarfsfall über die Polizei bei dieser Stelle beschweren könnten. Im letzten Absatz sicherte die Polizeibehörde den Bürgern zu: „Ihre Daten werden natürlich vertraulich behandelt." Ein Bürger, der von dieser Beschwerdemöglichkeit Gebrauch machte, war sehr erstaunt, als von dem Beamten, über den er sich beschwert hatte, eine Strafanzeige wegen Verleumdung gegen ihn erstattet wurde. Er wandte sich an den LfD und monierte, dass dieser Hinweis offensichtlich nicht ernst gemeint gewesen sei. Der LfD musste ihm Recht geben: zumindest dann, wenn Bürger ein persönliches Fehlverhalten von Polizeibeamten ansprechen, wird der betroffene Polizeibeamte regelmäßig Kenntnis über den konkreten Inhalt der vorgebrachten Beschwerde und auch über die Identität des Hinweisgebers erhalten müssen, da der Dienstherr nur so die Angelegenheit erfolgreich aufklären kann.

Auf Intervention des LfD wurde der Hinweis auf die Vertraulichkeit von Bürgerbeschwerden gegen Polizeibeamte im Internet ersatzlos gestrichen.

5.12.6 Versehentliche Versendung eines polizeilichen Rapports an den Presseverteiler

Eine Polizeiinspektion hatte versehentlich Lagedaten, die auch personenbezogene Daten von Beschuldigten, Zeugen, Geschädigten, Verkehrsunfallbeteiligten und verantwortlichen Personen beinhalteten, an den Presseverteiler übermittelt. Der LfD unterrichtete sich vor Ort über den Vorgang. Zwar wurde die Presse im Nachhinein um Datenlöschung gebeten, dennoch sahen sowohl der LfD als auch das Innenministerium Handlungsbedarf. Das ISM beabsichtigt, den Versand von Presseberichten nur noch über eine definierte Befehlsfolge innerhalb der Navigation „Presseberichte" zuzulassen. Dies ist eine aus der Sicht des LfD geeignete und ausreichende Maßnahme, um solche Versehen künftig noch unwahrscheinlicher werden zu lassen.

5.12.7 Löschung personenbezogener Daten infolge Berichtigung unzutreffender Informationen

Ein Petent, dem wiederholt durch eine Polizeibehörde keine oder unzureichende Auskünfte über zu seiner Person gespeicherte Daten erteilt wurden (vgl. 20. Tb., Tz. 5.11.1), ersuchte den LfD im Berichtszeitraum erneut um Unterstützung bei einem Auskunftsersuchen nach § 40 POG. Die Recherche des LfD ergab, dass aufgrund eines unzutreffenden POLADIS.net-Eintrages im Ereignisfeld eine zu lange Speicherdauer vergeben worden war. Der Empfehlung des LfD, die Daten unverzüglich zu löschen, wurde entsprochen.

5.12.8 Das Forschungsprojekt Foto-Fahndung im Mainzer Hauptbahnhof

Unter dem Arbeitstitel „Foto-Fahndung" hat das BKA im Zeitraum Oktober 2006 bis Ende Januar 2007 die biometrische Gesichtserkennung als neues Fahndungshilfsmittel für die Polizei im Mainzer Hauptbahnhof getestet. Dieser Test erregte bundesweit Aufsehen, weil befürchtet wurde, dass damit eine neue Qualität der Überwachung der Bürger vorbereitet werden sollte.

200 Pendler haben am Feldtest teilgenommen. Da zumindest kurzzeitig die Bilder aller Personen im Erfassungsbereich der Kameras gespeichert wurden, stellten sich durchaus datenschutzrechtliche Fragen. Verantwortlich für den Test war das BKA, das die Räumlichkeiten der Bahn nutzte. Damit war der LfD zur datenschutzrechtlichen Beurteilung der Angelegenheit nicht zuständig. Er teilte allerdings inhaltlich die hierzu veröffentlichte Auffassung des BfDI vollständig. Danach war das Projekt in Anwendung der Forschungsklausel des Bundesdatenschutzgesetzes zulässig (§ 14 Abs. 1, 2 Ziff. 9 BDSG).

Als Ergebnis der Untersuchungen kann festgehalten werden, dass es nur möglich ist, gesuchte Personen in Menschenmengen automatisch wiederzuerkennen, wenn die äußeren Rahmenbedingungen, insbesondere die Beleuchtung, stimmen. Da solche optimalen Bedingungen in der Praxis selten sind, war als Ergebnis festzustellen, dass die getesteten Verfahren noch nicht

praxistauglich sind. Den öffentlichen Abschlussbericht des BKA vom Februar 2007 kann jedermann im Internet herunterladen unter http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_abschlussbericht.pdf.

Es ist allerdings zu erwarten, dass künftig leistungsfähigere Systeme entwickelt werden, so dass die grundsätzliche Frage, ob und unter welchen Voraussetzungen ein solches Scannen von großen Personengruppen zu Fahndungszwecken zulässig sein soll, geklärt werden muss. Hier stellen sich vergleichbare Grundsatzfragen wie bei vielen anderen Recherchetechniken:

– Wieviel an Überwachung ist noch mit einem freiheitlichen Rechtsstaat, der seinen Bürgern nicht grundsätzlich misstraut, vereinbar?
– Sind die mit einem solchen Verfahren einhergehenden Eingriffe in die Rechte Unbeteiligter so schwerwiegend, dass die damit erreichbaren Fahndungserfolge und der mögliche Zugewinn an Sicherheit damit nicht erkauft werden sollten?

Diese Abwägung bleibt schwierig; sie muss letztlich unter Berücksichtigung aller relevanten Faktoren – auch nach Anhörung der Argumente der Datenschutzbeauftragten – verantwortlich vom Gesetzgeber getroffen werden.

5.13 Fußball-WM 2006

Wie bereits im 20. Tb. unter Tz. 5.9 berichtet, wurden im Rahmen der Vorbereitung und Durchführung der Fußballweltmeisterschaft 2006 eine Vielzahl personenbezogener Daten von Beteiligten sowie Zuschauern erhoben und verarbeitet. Deshalb richtete sich der datenschutzrechtliche Fokus im Berichtszeitraum neben den durch die Polizei getroffenen Vorbereitungen (Rahmenkonzeptionen und Vorfeldmaßnahmen) auf die Bewältigung verschiedenster Einsatzlagen (von dem Einsatz entsprechender Softwareprodukte über Livescan, Fast Identification, Videoüberwachungsmaßnahmen bis hin zur Einrichtung von Public Viewing Areas) und die Nachbereitung der Ereignisse. Durch die frühzeitige Einbindung des LfD konnte ein hohes Maß an Abstimmungen zwischen den beteiligten Polizeibehörden, Institutionen und Einrichtungen insbesondere hinsichtlich der datenschutzrechtlichen Anforderungen erreicht werden.

5.13.1 Datenschutzfragen im Zusammenhang mit der Akkreditierung

Ohne besondere gesetzliche Grundlage wurden im Rahmen des Akkreditierungsverfahrens anlässlich der Fußballweltmeisterschaft 2006 Zuverlässigkeitsprüfungen durch Polizei und Verfassungsschutz durchgeführt. Ein vergleichbares Verfahren fand auch anlässlich des Papstbesuchs 2006 in Bayern Anwendung. Grundlage für die Einbeziehung der Betroffenen war deren zuvor abgegebene schriftliche Einwilligung. In diesen Fällen wurden von der Mehrheit der Datenschutzbeauftragten im Hinblick auf die Besonderheit der Ereignisse keine grundsätzlichen Einwendungen erhoben. Sollte dieses Verfahren aber Schule machen, ist aus der Sicht der Mehrheit der Datenschutzbeauftragten eine Entscheidung des Gesetzgebers über das „ob“ und das „wie“ einer solchen Zuverlässigkeitsprüfung notwendig. Auch dann müssen diese Zuverlässigkeitsprüfungen auf wirklich sicherheitsempfindliche Großereignisse beschränkt bleiben.

Landesweit überprüfte die Polizei im Rahmen der WM-Akkreditierung 6.878 Datensätze. Davon wurden 59 Anträge wegen Vorliegens polizeilicher Erkenntnisse zurückgewiesen. In zwei Fällen konnten ablehnende Voten zurückgenommen werden (Umvotierungen). Von den insgesamt 66 beantragten führte eine Tagesakkreditierung zu einem ablehnenden Votum. Nach Abschluss des Akkreditierungsverfahrens wurden die Unterlagen der einzelnen Ablehnungsfälle zur Dokumentation der Ablehnungsgründe für die Dauer eines Jahres bei dem behördlichen Datenschutzbeauftragten des LKA archiviert und (nachdem bisher keine Eingaben der Betroffenen erfolgten) mit Stand vom Juli 2007 vernichtet. Die Prüfung des LfD ergab, dass bei der Bearbeitung der Anträge sorgfältig vorgegangen, nachvollziehbare Voten abgegeben wurden und eine datenschutzgerechte Wertung erfolgte. Dazu ist anzumerken, dass zum Zeitpunkt der Prüfung der LfD die Auffassung vertrat, das Polizei- und Ordnungsbehördengesetz biete für diese Art der Datenverarbeitung eine ausreichende Rechtsgrundlage. Ob dies vor dem Hintergrund der vom Bundesverfassungsgericht in seiner aktuellen Rechtsprechung formulierten Anforderungen an das Vorliegen einer konkreten Gefahr künftig aufrecht zu erhalten ist, ist zweifelhaft. Der LfD beabsichtigt, diese Frage in weiteren Erörterungen mit dem Innenministerium zu klären.

5.13.2 Datenschutzfragen im Zusammenhang mit der Nutzung spezieller polizeilicher Verfahren zur Einsatzbewältigung

Die bei der Fußballweltmeisterschaft 2006 eingesetzte Einsatzsoftware diente Dokumentationszwecken und der Informationssteuerung. Es wurden überwiegend Daten von Personen gespeichert, die von freiheitsbeschränkenden Maßnahmen wie beispielsweise einem Platzverweis oder einem Aufenthaltsverbot betroffen waren. Insgesamt umfasste die Speicherung 7.243 Datensätze, davon 316 Personalieneinträge. Die Polizei griff die Anregung des LfD auf, die Daten nach Ereignisende zunächst zu sperren und für bestimmte Auswertungszwecke maximal drei Monate vorzuhalten sowie Zugriffsrechte auf einige wenige Anwender, deren Aktivitäten nachvollzogen werden können, zu beschränken.

5.13.3 Videoüberwachung

In Ergänzung der Ausführungen im 20. Tb. (Tz. 5.9) ist festzustellen, dass insgesamt 38 Videokameras zur Überwachung des Stadtgebietes von Kaiserslautern einschließlich der so genannten Fanmeile und der Public-Viewing-Areas installiert worden waren. Unmittelbar nach Abschluss der Fußballweltmeisterschaft wurde mit dem Abbau von 28 dieser Videoüberwachungsanlagen begonnen. Gleiches gilt (wegen der hohen Folgekosten) für die zur Verkehrsüberwachung genutzten und von der Stadt Kaiserslautern installierten 53 Videokameras. Elf Kameras, die entlang des Weges von der Logenstraße (Bahnhofsnähe) zum Fritz-Walter-Stadion angebracht sind, werden derzeit ausschließlich bei Bundesliga- oder DFB-Pokalspielen im offenen Einsatz genutzt. Von den im Innenbereich des Stadions (Tribünenbereich, Funktionsräume) und unmittelbar an der Gebäudeaußenseite durch die Stadionbetreibergesellschaft installierten 106 Kameras verblieben 81 für die weitere Nutzung. Im wesentlichen ergaben sich im Zuge des Einsatzes der Videoaufzeichnungsanlagen datenschutzrechtliche Prüfungsansätze hinsichtlich der Kennzeichnung (Größe der in Kaiserslautern installierten Hinweisschilder), der Erkennbarkeit des aktiven Betriebs von Videoüberwachungsgeräten (Kamera ist aktiviert), und der Überwachung privaten Wohnraums.

5.13.3.1 Hinweise auf die Videoüberwachung

Petenten führten Beschwerde darüber, dass an vielen Kamerastandorten in Kaiserslautern entweder nur kleine (ca. 10 x 7 cm) Aufkleber an den Befestigungsmasten der Kameras oder aber größere (DIN A4-Format) in großer Höhe (ca. 3 m) so angebracht worden seien, dass nur durch gezieltes Suchen bzw. erst nach Durchquerung des überwachten Bereichs die Kameras hätten entdeckt werden können. Außerdem seien keine Informationen darüber vorhanden gewesen, welche Bereiche wann überwacht werden und ob die Kameras ein- oder ausgeschaltet seien. Die datenschutzrechtliche Prüfung umfasste zunächst die Bewertung, ob die in Kaiserslautern mittels Aufzeichnungsgeräten überwachten Örtlichkeiten im Sinne des § 27 Abs. 7 POG bzw. § 6 b Abs. 2 BDSG, § 34 Abs. 2 LDSG so deutlich gekennzeichnet waren, dass jedermann vor Betreten dieser Areale eine hinreichende Möglichkeit zur Kenntnisnahme hatte. Ergebnis der vom LfD vor Ort vorgenommenen Überprüfung war, dass die Installation noch nicht abgeschlossen, aber bereits eine Vielzahl von der DIN 33450 entsprechenden, 0,20 m x 0,20 m großen Videoinformationszeichen in einer Höhe von ca. 3 m an Lichtmasten oder Verkehrszeichen angebracht worden waren. Auf die verantwortliche Stelle wurde durch die Schriftzüge „Polizei Kaiserslautern“, „Stadt Kaiserslautern, Technische Werke Kaiserslautern (TWK)“, „FIFA“ hingewiesen. Insoweit hatte der LfD den Eindruck gewonnen, dass nach Installation aller Kameras und Videoinformationszeichen auch für den Ortsunkundigen die Möglichkeit bestand, vor Betreten der überwachten Areale auf die Videokameras aufmerksam zu werden.

Hinsichtlich der Bekanntgabe geplanter Videoüberwachungsmaßnahmen hatten die Recherchen ergeben, dass die Polizei Kaiserslautern die Bürger (insbesondere die Anwohner der Überwachungsbereiche der Innenstadt und des Betzenbergs) in insgesamt fünf öffentlichen Veranstaltungen über die Videoüberwachung informiert hatte. Darüber hinaus waren einige besonders betroffene Anwohner direkt angesprochen worden. Insoweit hatte die Polizei den datenschutzrechtlichen Anforderungen entsprochen. Anders war hingegen der Einwand zu beurteilen, es sei nicht zu erkennen, ob eine Kamera ein- oder abgeschaltet sei. Diesbezüglich prüfte die Polizei Kaiserslautern auf Empfehlung des LfD, wie die temporäre Nutzung der Kameras, die nach der Weltmeisterschaft bei Bundesligaspielen im offenen Einsatz genutzt werden sollen, Passanten verdeutlicht werden könnte. Neben technischen Lösungen wurde die Möglichkeit des Anbringens von Zusatzschildern, beispielsweise mit der Aufschrift „Videoüberwachung nur bei Fußballspielen“ beraten. Dies wäre aus datenschutzrechtlicher Sicht ausreichend. Inzwischen sind entsprechende Schilder, die den Datenschutzanforderungen entsprechen, angebracht worden.

5.13.3.2 Erfassungsbereich der Videokameras

Im Zuge der Vorbereitungen zur Fußballweltmeisterschaft 2006 waren Überwachungskameras installiert worden, deren Wirkbereich 360 Grad umfasste. Dies hatte in einem Fall dazu geführt, dass sowohl ein Fenster einer Erdgeschosswohnung als auch der Garten des Anwesens im Schwenkbereich der Kamera lag. Aus datenschutzrechtlicher Sicht ist zwar vom Grundsatz her die Erhebung personenbezogener Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen gemäß § 27 Abs. 2 POG bei oder im Zusammenhang mit öffentlichen Veranstaltungen zulässig, doch ist auch dies auf das absolut Notwendige zu beschränken. Der Schutz der Individualsphäre der Petenten konnte im Zusammenwirken mit der Polizei dadurch gewährleistet werden, dass „Privacy Zones“ durch Schwärzung von Teilen des Erfassungsbereichs der Kameras berücksichtigt wurden.

5.14 Internationale Zusammenarbeit der Polizei und Datenschutz

5.14.1 Fehlende Regelungen auf europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit der Frage des Datenschutzes bei der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene befasst (71. Konferenz vom 16. und 17.3.2006 in Magdeburg; Entschließung „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen"; s. Anlage 11). Sie mahnt darin u.a. die Schaffung verbindlicher normenklarer Regelungen an, die insbesondere die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleisten müssten. An Drittstaaten dürften Daten nur dann weitergegeben werden, wenn dort ein angemessener Datenschutz sichergestellt sei.

5.14.2 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

Ebenso hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder u.a. auch auf Initiative des rheinland-pfälzischen LfD mit dem Problem der Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige befasst (s. Entschließung „Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige" der 71. Konferenz vom 16.-17.3.2006 in Magdeburg; Anlage 9). Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen. Die Listen sind öffentlich; es handelt sich dabei um eine verschärfte Form eines modernen Prangers.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in dieser Entschließung die Bundesregierung aufgefordert, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen; diese werden bislang nicht ausreichend gewahrt, da Betroffene nahezu keine wirksamen Instrumente haben, die Berechtigung ihrer Eintragung in einer solchen Liste gerichtlich überprüfen zu lassen.

6. Verfassungsschutz

6.1 Vorbemerkung

Die Kontrolle von Eingriffen in das Brief-, Post- und Fernmeldegeheimnis durch den Landesverfassungsschutz gemäß § 1 Abs. 1 Nr. 1 und § 10 Abs. 1 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298) ist den Befugnissen des LfD gesetzlich entzogen. Zur Kontrolle von entsprechenden Beschränkungen hat der Landtag eine Kommission (G 10-Kommission) gebildet. Diese entscheidet über die Zulässigkeit und Notwendigkeit der Anordnung, Durchführung und Fortdauer solcher Beschränkungsmaßnahmen der Landesverfassungsschutzbehörde (§ 2 des Landesgesetzes zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 16.12.2002, GVBl 2002, S. 477). Erkenntnisse über diese Tätigkeit des Verfassungsschutzes hat der LfD also nur, soweit sie allgemein zugänglichen Quellen entnommen werden können.

Zusätzlich zu den Kontrollbefugnissen des LfD hat die Parlamentarische Kontrollkommission des Landtags gem. § 20 LVerfSchG Kontrollaufgaben. Sie nimmt das parlamentarische Kontrollrecht hinsichtlich der Tätigkeit der Verfassungsschutzbehörde wahr. Ihre Beratungen sind geheim, ihre Mitglieder sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen im Rahmen ihrer Tätigkeit bekannt werden. Der zuständige Minister unterrichtet sie mindestens zweimal jährlich umfassend über die allgemeine Tätigkeit der Verfassungsschutzbehörde und über Vorgänge von besonderer Bedeutung. Die Unterrichtung umfasst auch den Einsatz der akustischen Wohnraumüberwachung; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten dieser Maßnahmen zu geben.

Damit ist eine regelmäßige parlamentarische Kontrolle gegeben. Der LfD hat auch vor diesem Hintergrund und wegen fehlender personeller Ressourcen im Berichtszeitraum in diesen Bereichen keine Kontrollen durchgeführt.

Das Landesgesetz zur Neufassung des Ausführungsgesetzes zu Art. 10 GG und zur Fortentwicklung verfassungsschutzrechtlicher Vorschriften vom 16.12.2002 sah vor, dass die dem Terrorismusbekämpfungsgesetz des Bundes entsprechenden Erweiterungen der Eingriffsmöglichkeiten der Verfassungsschutzbehörde (s. Tz. 6.1.1 des 19. Tb.) bis zum 10.1.2007 befristet sind. Mit dem Gesetz zur Änderung des Gesetzes zur Neufassung des Ausführungsgesetzes zu Art. 10 GG und zur Fortentwicklung verfassungsschutzrechtlicher Vorschriften vom 19.12.2006 hat der Landesgesetzgeber eine erste Verlängerung dieser Frist bis zum 10.1.2008 beschlossen. Als Grund für diese Verlängerung hat die Landesregierung angegeben, dass im Interesse der Funktions-

fähigkeit des Bund-Länder-Verfassungsschutzverbundes die Evaluierung des Bundesrechts abgewartet werden sollte, um anschließend eigene Anschlussregelungen treffen zu können. Durch die zwischenzeitlich mit dem Terrorismusbekämpfungsergänzungsgesetz des Bundes begonnene Fortentwicklung des Verfassungsschutzrechts sieht sich die Landesregierung in dieser Vorgehensweise grundsätzlich bestätigt. Wie die aktuelle rechts- und sicherheitspolitische Diskussion zur offensiven Nutzung des Internets und insbesondere zum verdeckten Zugriff auf informationstechnische Systeme zeige, sei diese Fortentwicklung aber noch nicht abgeschlossen. Erst nach einer diesbezüglichen Entscheidung des Bundesverfassungsgerichts zum nordrhein-westfälischen Verfassungsschutzgesetz stehe zu erwarten, dass sowohl beim Bund als auch in den Ländern verfassungskonforme Regelungen dazu möglich würden. Damit Rheinland-Pfalz auf diese Entwicklung reagieren könne und bis dahin eine wirkungsvolle Bekämpfung des internationalen Terrorismus gewährleistet sei, solle die vorgesehene Frist nochmals verlängert werden. Um dem Landesgesetzgeber die Möglichkeit zu geben, nach der Entscheidung des Bundesverfassungsgerichts und der darauf folgenden Verabschiedung von Regelungen auf Bundesebene angemessene Folgeänderungen auch des Landesrechts zu beschließen, soll die Fristverlängerung zwei Jahre betragen.

Ein entsprechendes Gesetz war im Zeitpunkt des Berichtsabschlusses in Vorbereitung. Aus der Sicht des LfD ist diese Verlängerung akzeptabel.

6.2 Auskunftserteilungen bzw. -verweigerungen durch die Verfassungsschutzbehörde

§ 18 LVerfSchG regelt die Auskunft an Betroffene wie folgt:

Die Verfassungsschutzbehörde erteilt Betroffenen über zu ihrer Person in Akten und Dateien gespeicherte Daten sowie über den Zweck und die Rechtsgrundlage für deren Verarbeitung auf Antrag unentgeltlich Auskunft. Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und auf die empfangende Stelle bei Übermittlungen. Über personenbezogene Daten in nicht automatisierten Dateien und Akten, die nicht zur Person von Betroffenen geführt werden, ist Auskunft nur zu erteilen, soweit Angaben gemacht werden, die ein Auffinden der personenbezogenen Daten mit angemessenem Aufwand ermöglichen. Ein Recht auf Akteneinsicht besteht nicht (§ 18 Abs. 1 LVerfSchG).

Die Auskunftserteilung unterbleibt, soweit durch sie eine Gefährdung der Aufgabenerfüllung zu besorgen ist, durch sie Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise der Verfassungsschutzbehörde zu befürchten ist, sie die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen Dritter geheimgehalten werden müssen (§ 18 Abs. 2 LVerfSchG).

Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Wird die Auskunftserteilung abgelehnt, sind Betroffene auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an die Datenschutzbeauftragten wenden können. Mitteilungen des Datenschutzbeauftragten an Betroffene dürfen keine Rückschlüsse auf den Erkenntnisstand der Verfassungsschutzbehörde zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat (§ 18 Abs. 3 LVerfSchG).

Vor diesem rechtlichen Hintergrund haben sich mehrere Bürger an den LfD gewandt, deren Auskunftsersuchen vom Verfassungsschutz unter Hinweis auf die oben genannten Hinderungsgründe ohne nähere Begründung abgelehnt worden war. Der LfD hat in diesen Fällen regelmäßig überprüft, ob die beim Verfassungsschutz vorhandenen Daten zulässigerweise erhoben und gespeichert worden sind. Der Verfassungsschutz hat bereitwillig an diesen Überprüfungen mitgewirkt und die Aufgabenerfüllung des LfD unterstützt. Gelegentlich konnte auch den Betroffenen in enger Abstimmung mit dem Verfassungsschutz Genaueres über die vorhandenen Speicherungen – oder auch das Fehlen von Speicherungen – mitgeteilt werden. Insgesamt haben sich aus der Sicht des LfD die gesetzliche Auskunftsregelung und das bisher praktizierte Verfahren in diesem Bereich bewährt.

7. Justiz

7.1 Vorbemerkung

Der LfD besitzt im Bereich der Justiz nur soweit Zuständigkeiten, wie es um die „Justizverwaltung“ geht. Soweit damit die Unabhängigkeit der Richter geschützt werden soll und externe Einflüsse auf die Rechtsprechenden ausgeschlossen werden, ist diese Beschränkung verfassungsrechtlich geboten.

Soweit Fragen der richterlichen Unabhängigkeit nicht betroffen sind, bewegt sich der LfD aber aus seiner Sicht im Bereich der Justizverwaltung im Sinne des Datenschutzgesetzes. Er hält sich für verpflichtet, auch hier auf die Beachtung der datenschutzrechtlichen Regelungen hinzuweisen. Grundlegende Konflikte haben sich in der Praxis im Berichtszeitraum nicht ergeben, allerdings konnte nicht in allen Punkten Übereinstimmung erzielt werden (s. beispielsweise unten Tz. 7.3.1.1).

7.2 Strafrecht/Strafverfahrensrecht

7.2.1 Genomanalyse im Strafverfahren

Die Bundesregierung sowie die Koalitionsfraktionen haben ein „Gesetz zur Novellierung der forensischen DNA-Analyse“ in den Deutschen Bundestag eingebracht, das am 1.11.2005 in Kraft getreten ist (BGBl. I S. 2360). Die Neuregelung senkt die Schranken für DNA-Analysen in laufenden Ermittlungsverfahren (§§ 81e, 81f StPO) sowie zur Identitätsfeststellung in künftigen Strafverfahren (§ 81g StPO) deutlich ab. Im Gesetzgebungsverfahren haben sich die Datenschutzbeauftragten geäußert. Ihren Anregungen und Bedenken wurde jedoch nicht Rechnung getragen.

Die DNA-Analyse ist nunmehr auch auf Grundlage einer Einwilligung des Betroffenen möglich. Einwilligungen sind nur wirksam, wenn sie freiwillig erfolgen. Da der Betroffene sich im Strafverfahren regelmäßig in einer besonderen Drucksituation befindet, bestehen Zweifel, ob auf dieser Grundlage überhaupt in nennenswertem Maß DNA-Analysen erfolgen können. Hinzu kommt bei einer Einwilligung in DNA-Analysen zur Identitätsfeststellung in künftigen Strafverfahren, dass der Betroffene sich gewissermaßen selbst die erforderliche Negativprognose im Hinblick auf die Begehung künftiger Straftaten stellen müsste, was ihm kaum zugemutet werden kann. Eine weitere Schwächung des Richtervorbehalts liegt in der neu eingeführten Eilfallkompetenz für Staatsanwaltschaft und Polizei. Für diese Regelung fehlt es an rechtstatsächlichen Anhaltspunkten dafür, dass gerade durch die Notwendigkeit der Einschaltung eines Richters in Eilfällen DNA-Analysen nicht rechtzeitig durchgeführt werden können. Keine Einwände bestanden gegen die erfolgte Abschaffung des Richtervorbehalts für die molekulargenetische Untersuchung von unbekanntem Spurenmaterial.

Für DNA-Analysen zur Identitätsfeststellung in künftigen Strafverfahren werden durch die Neuregelung auch die Anforderungen an die Anlasstaten und die zu prognostizierenden künftigen Straftaten des Betroffenen herabgesetzt. Für beides waren bislang Straftaten von erheblicher Bedeutung bzw. Sexualstraftaten erforderlich. Nunmehr kann jeweils auch die wiederholte Begehung nicht erheblicher Straftaten (z.B. Sachbeschädigung, Hausfriedensbruch) genügen, wenn dies im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichsteht.

Zu begrüßen ist, dass für das DNA-Massenscreening („Massengentest“) auf freiwilliger Basis jetzt eine ausdrückliche gesetzliche Grundlage geschaffen wurde (§ 81h StPO). Dies entspricht der Forderung der Datenschutzbeauftragten nach einer klarstellenden gesetzlichen Festlegung der rechtlichen Rahmenbedingungen dieses Ermittlungsinstruments. Zur Anwendung dieser Regelung haben die Datenschutzbeauftragten Empfehlungen formuliert, die die Berücksichtigung des Verhältnismäßigkeitsgrundsatzes sicherstellen sollen. Im Land ist es nach Kenntnis des LfD noch nicht zu spektakulären Massengentests gekommen.

Das Gesetz zur Novellierung der forensischen DNA-Analyse ist nach zwei Jahren (also Ende 2007) zu evaluieren und im Rahmen dessen ist auch zu prüfen, ob die DNA-Analyse aus kriminalpolitischen Gründen anders als bislang geregelt werden muss. Die Datenschutzbeauftragten werden dies aufmerksam mit dem Ziel angemessener Lösungen begleiten.

7.2.2 Bundesgesetz zur Neuregelung der Telekommunikationsüberwachung

Die Bundesregierung will die rechtlichen Regelungen zu den verdeckten strafprozessualen Ermittlungsmaßnahmen überarbeiten und in einem Gesamtsystem vereinheitlichen (Gesetzentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drs. 275/07). Dabei sollen höchstrichterliche Vorgaben umgesetzt und zugleich neue technische Entwicklungen berücksichtigt werden. Die Ausgestaltung der verdeckten – also für den davon Betroffenen nicht erkennbaren – Ermittlungsmethoden soll grundrechtssicher – unter Berücksichtigung des verfassungsrechtlich gebotenen Schutzes des Kernbereichs der persönlichen Lebensgestaltung – erfolgen, der Rechtsschutz gegen solche Maßnahmen soll verstärkt werden. Der Entwurf will zudem die europarechtlichen Vorgaben zur Erfassung der Telekommunikationsverbindungsdaten zum Zweck der Strafverfolgung in nationales Recht umsetzen.

Die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 8.-9.3.2007 in Erfurt dazu eine Entschließung mit dem Titel „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen“ gefasst (s. Anlage 18), in der sie Nachbesserungen des Gesetzes gefordert hat. In Widerspruch dazu hatten Fachausschüsse des Bundesrats diesem eine umfangreiche Stellungnahme mit über 50 Einzeländerungsvorschlägen,

Prüfbitten und redaktionellen Hinweisen dazu zugeleitet, die zu einer Erweiterung und Erleichterung der Eingriffsmaßnahmen führen sollten (Ausschussempfehlungen Drs. 275/1/07 zu Drs. 275/1/0).

- Gefordert wurde unter anderem, den Katalog der Anlasstaten für die Telekommunikationsüberwachung zu erweitern. So müssten die Überwachungsmaßnahmen unter anderem auch zur Bekämpfung des Dopings im Sport eingesetzt werden.
- Die Ausschüsse verlangten, dass die Speicherdauer für die im Entwurf vorgesehene Verpflichtung der Telekommunikationsunternehmen, die Verkehrsdaten ihrer Kunden zu speichern, von sechs Monaten auf ein Jahr verlängert werde.
- Die Anbieter sollten Auskünfte auch dann erteilen müssen, wenn sie zur Durchsetzung von Urheberrechten oder zur Ermittlung von Zeugen notwendig seien.
- Zudem wurde gefordert, die so genannte verdeckte Online-Durchsuchung von Computern zur Bekämpfung insbesondere von terroristischen Vereinigungen und organisierter Kriminalität zu ermöglichen.
- Außerdem sollte die Dauer der Anordnung oder Verlängerung von Überwachungsmaßnahmen von zwei auf drei Monate verlängert werden können.
- Daten, die einem prozessualen Beweiserhebungs- oder -verwertungsverbot unterfallen, sollten nicht sofort gelöscht, sondern lediglich gesperrt werden, damit sie nicht unwiederbringlich verloren gehen, sondern nach einem möglichen Wegfall des Verwertungsverbots noch nutzbar seien. Geklärt werden müsse, wie diese Daten – insbesondere solche, die den Kernbereich privater Lebensgestaltung betreffen – herausgefiltert werden können, ohne gleich den ganzen Aufzeichnungsvorgang zu löschen.

Der LfD hat von diesen Vorschlägen erst sehr kurzfristig vor der maßgeblichen Sitzung des Bundesrats erfahren. Er ist diesen Vorschlägen, die zu datenschutzrechtlichen Verschlechterungen führen würden, deutlich entgegen getreten. Das Ministerium der Justiz hat mitgeteilt, dass es in weitem Umfang diese Vorschläge im Bundesrat nicht unterstützt habe.

Das Gesetzgebungsverfahren ist derzeit noch nicht abgeschlossen.

7.2.3 Online-Durchsuchungen von Computerfestplatten verdächtiger Personen

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen Sicherheitspolitiker und staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ oder sonstiger spezieller Software heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten. Es besteht Einvernehmen, dass dies nur auf der Grundlage einer ausdrücklichen gesetzlichen Regelung zulässig sein kann. Zurzeit wird diskutiert, das BKAG entsprechend zu ergänzen. Aber es ist auch zu erwarten, dass die StPO und – auf der Ebene des Landes – das POG sowie das Landesverfassungsschutzgesetz in gleicher Weise ergänzt werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung (vom 8.-9.3.2007, „Keine heimliche Online-Durchsuchung privater Computer“, 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Erfurt, vgl. Anlage 19) einmütig dagegen gewandt. Sie haben entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl für die Strafverfolgung wie für die Gefahrenabwehr Stellung genommen und an die Gesetzgeber appelliert, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Es müsse ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden dürfe. Die Konferenz befürchtet zudem massive Sicherheitseinbußen, weil zu erwarten sei, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit würden aber auch die sicherheitstechnisch wichtigen Softwareupdates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde weiterhin das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert.

Die Diskussion um die gesetzliche Einführung der Online-Durchsuchung war im Zeitpunkt der Berichterstattung noch nicht abgeschlossen. Der LfD hat es vor dem Hintergrund der absehbaren Entwicklung der Gesetzgebung zum Thema „Online-Durchsuchung“ für erforderlich gehalten, die Position der Datenschutzbeauftragten, die sie in ihrer oben wiedergegebenen Entschließung zum Ausdruck gebracht haben, fortzuschreiben bzw. zu aktualisieren. Eine Äußerung zu den zu erwartenden gesetzgeberischen Initiativen setzt seiner Auffassung nach voraus, dass fundierte Kenntnisse über das von den Bedarfsträgern (in erster Linie vom BKA) Gewünschte und für erforderlich Gehaltene, ihre hier verfolgten Ziele sowie über die technische Situation in diesem Zusammenhang, über das technisch Mögliche und Machbare und über etwa bestehende Gefahren gewonnen werden. Seine Bemühungen, hierzu auf der Ebene des Landes Erkenntnisse zu gewinnen, sind bislang vor allem deshalb wenig erfolgreich geblieben, weil das Know-how auf diesem Gebiet primär beim BKA zu verorten ist. Auch die Szenarien und Fallgestaltungen, für deren Bewältigung solche „Online-Durchsuchungen“ gewünscht werden, werden in erster Linie dort

diskutiert. Vor diesem Hintergrund hat er sich darum bemüht, im Kontakt mit dem BfDI insbesondere folgende Fragen zu klären:

- Welche konkreten Defizite bestehen im Rahmen der Prävention und der Strafverfolgung, die nur mit Hilfe eines neuen gesetzlichen Instruments der „Online-Durchsuchungen“ behoben werden können? Mit anderen Worten: Welche Nutzung der EDV durch Straftäter oder Gefährder ist den Gefahrenabwehr- bzw. den Strafverfolgungsbehörden bislang nicht zugänglich? Aus welchen Gründen reichen die herkömmlichen Eingriffsgrundlagen (insbesondere die Regelungen über Durchsuchung und Beschlagnahme sowie über die Eingriffe in das Telekommunikationsgeheimnis) nicht aus? An welche Szenarien wird dabei konkret gedacht?
- Welche technischen Verfahrensweisen sollen zur Durchführung von „Online-Durchsuchungen“ konkret eingesetzt werden? Soll der Weg über sog. „Remote Forensic Software“ (RFS) gewählt werden und soll die Software unmittelbar unter Zugriff auf den Rechner – nicht online – installiert werden oder welche Wege mit welchen spezifischen Risiken würden genutzt werden (vgl. hierzu heise news v. 3.8.2007, ‚Bundestrojaner‘ heißt jetzt angeblich ‚Remote Forensic Software‘)? Sind mit dem Einsatz dieser Verfahrensweisen Gefahren für den technisch-organisatorischen Datenschutz der Nutzer verbunden, die über die konkrete Eingriffsmaßnahme hinaus Bedeutung haben? Können solche Folgen verhindert werden, ggf. wie?
- Gibt es die Möglichkeit, den Kernbereich der persönlichen Lebensgestaltung etwa durch technisch-organisatorische Vorkehrungen bei „Online-Durchsuchungen“ zu schützen oder zumindest die Gefahr zu minimieren, dass bei entsprechenden Maßnahmen in diesen Kernbereich eingedrungen wird? Welche Verfahrensweisen wären ggf. geeignet, diesen Schutz zu ermöglichen?

In diesem Zusammenhang haben auch die FDP-Bundestagsfraktion mit detaillierten Fragen in ihrer Kleinen Anfrage v. 10.4.2007 (BT-Drs. 16/4887) sowie die SPD-Bundestagsfraktion (Fragenkatalog der AGs Kultur und Medien sowie Neue Medien für eine Anhörung des Bundesinnenministeriums am 27.8.2007 in Berlin (https://tepin.aiki.de/blog/archives/159-SPD-hat-45-Fragen-zur-Online-Durchsuchung.html) sich um Klärungen bemüht. Diese Klärungsbemühungen dauern derzeit an.

7.2.4 Einsatz von Handys als Abhör- und Ausforschungsinstrument

Dem LfD ist bekannt geworden, dass auf dem Markt ein Softwarewerkzeug frei erhältlich ist, das es erlaubt, ein entsprechend präpariertes Handy vielfältig zur Ausforschung des Nutzers zu verwenden. Zu den vom Anbieter im Internet genannten Funktionen gehören:

- Entfernt Mithören: das Handy könne unbemerkt eingeschaltet werden und ermögliche in seiner Umgebung das Mithören. Dies erfolge allerdings nur, wenn das Handy nicht in Gebrauch sei.
- Fernbedienung durch SMS: Alle Funktionen der Software könnten entfernt durch SMS ein- und ausgeschaltet werden. Außer der Basiskonfiguration sei kein Zugang zum Apparat erforderlich.
- SMS protokollieren: Alle vom Handy empfangene oder geschickte SMS könnten online gelesen werden. Alle Sprachen würden unterstützt.
- Anrufsgeschichte: Anfangszeit und Nummer aller Anrufe würden übermittelt. Wenn das Handy die Nummer im Adressbuch habe, werde der Name gezeigt.
- Gesprächsdaueranzeige: Anzeige, wie lange ein Anruf gedauert habe.
- Private Daten löschen: durch SMS-Kommando könnten alle privaten Fotos, Kontakte, SMS, E-Mail, MMS entfernt werden.
- Freie Datensuche ermögliche es, die Daten des Handys auf Stichwörter, Datum, Typ usw. zu durchsuchen.
- Protokolle downloaden: Download der Datenprotokolle und Suchergebnisse als CSV, RTF oder PDF sei möglich.
- SMS, wenn SIM ersetzt wird: Wenn die SIM-Karte des Handy ersetzt werde, erfolge eine Nachricht über die neue Karte durch SMS.

Diese Informationen lassen sich der Website des Anbieters im Internet entnehmen (http://www.flexispy.com/de/products_compare.html). Anbieter ist eine thailändische Firma, die nach den Internetangaben eine Niederlassung in London hat.

In der Presse wurde darüber wie folgt berichtet: „Handys können ihre Besitzer belauschen;... ‚Flexispy‘ (engl. = flexibler Spion) heißt das Spionageprogramm, das mittlerweile auch in Deutschland vom thailändischen Hersteller ganz offen beworben wird. Dr. Wilhelm Pütz, Abhörexperte beim Bundesamt für Sicherheit in der Informationstechnik (BSI): Der ‚Spion‘ muss das fremde Handy nur ein paar Minuten in die Hand bekommen. Dann kann er eine Speicherkarte mit dem Spionageprogramm ins Handy einlegen und die Software mit wenigen Tastenbefehlen dort installieren. Auch die Justiz hat die neuen technischen Möglichkeiten für sich entdeckt. Laut ‚Spiegel‘ werden Handys bereits in mehreren Ermittlungsverfahren als Wanze eingesetzt.“ (Bild 18.7.2007 S. 11).

Der LfD hat deshalb das Ministerium der Justiz sowie das Innenministerium befragt. In ihrer gemeinsamen Antwort stellten sie fest, dass die oben genannte Funktion des „Entfernt Mithörens“ mit dieser Software nicht möglich sei. Das Programm sei im Geschäftsbereich des Justizministeriums zur Strafverfolgung nicht genutzt worden; auch sonstige heimliche Umprogrammierungen von Handys insbesondere mit dem Ziel umfangreicher Abhörmaßnahmen seien nicht erfolgt. Das Justizministerium hält es für zweifelhaft, ob derzeit ein gesetzliches Verbot des freien Vertriebs dieses Produkts in Deutschland besteht. Der konkrete Einsatz zu illegalen Abhörzwecken stehe dagegen unter Strafdrohung. Zur Situation auf der Ebene des Bundes s. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE, BT-Drs. 16/6328 vom 27.9.2007. Der LfD unterstützt die Bemühungen des BfDI, hier Strafbarkeitslücken zu schließen (vgl. den 21. Tb. des BfDI, Tz. 6.4, S. 90).

7.2.5 Haus des Jugendrechts in Ludwigshafen

Am 1.9.2005 wurde das „JuReLu – Ludwigshafener Haus des Jugendrechts“ eröffnet. Sein zentrales Anliegen ist es, die Verfahrensabläufe bei der Verfolgung und Verhütung von Jugendkriminalität durch die Zusammenführung von Polizei, Staatsanwaltschaft, Jugendgerichtshilfe sowie dem pfälzischen Verein für Straffälligenhilfe „unter einem Dach“ zu optimieren. Das Polizeipräsidium Rheinpfalz setzt 15 Polizeibeamtinnen und -beamte von Schutz- und Kriminalpolizei sowie eine Polizeiverwaltungsangestellte im „Haus des Jugendrechts“ ein, die dort zentral die Aufgaben der Verfolgung und Verhütung von Jugendkriminalität im Stadtgebiet Ludwigshafen wahrnehmen. Die Staatsanwaltschaft Frankenthal hat zwei Jugenddezernenten für die Arbeit im „Haus des Jugendrechts“ eingesetzt, die dort ein Büro haben. Es wurde das sog. Wohnortprinzip eingeführt; die polizeiliche Zuständigkeit bestimmt sich nicht mehr nach dem Tatort, sondern nach dem Wohnort des Jugendlichen. Dadurch wurden die Organisation der Staatsanwaltschaft und des Jugendamtes aneinander angeglichen. Im Regelfall entwickeln die Sachbearbeiter der Polizei und der Jugendgerichtshilfe in einer „kleinen Fallkonferenz“ einen gemeinsamen Vorschlag, den sie der letztlich entscheidenden Staatsanwaltschaft unterbreiten. Insbesondere bei Mehrfach- bzw. Wiederholungstätern findet unter dem Vorsitz der Staatsanwaltschaft eine sog. „große Fallkonferenz“ der beteiligten Institutionen zur Abstimmung eines effektiven Handlungskonzeptes statt. Im Jahr 2006 wurden dort insgesamt 3.280 Ermittlungsverfahren bearbeitet.

Aus datenschutzrechtlicher Sicht ist es vorrangig, zu gewährleisten, dass durch die enge räumliche Zusammenarbeit der verschiedenen Institutionen nicht Datenübermittlungen erfolgen oder Datenzugriffsmöglichkeiten geschaffen werden, die durch die Rechtslage nicht gedeckt sind. Insbesondere ist der Schutz des Sozialgeheimnisses auch in diesem Rahmen zu wahren. Die Schaffung einer gemeinsamen Geschäftsstelle für alle im Haus ansässigen Stellen unter Einschluss eines privatrechtlichen Vereins ist aus dieser Sicht problematisch. Der LfD hat anlässlich örtlicher Feststellungen auf diesen Gesichtspunkt hingewiesen. Es wurde zugesichert, dass entsprechende organisatorische Vorkehrungen zur Wahrung der gesetzlich gebotenen Beachtung von Datenübermittlungsregelungen getroffen werden. Da das Ludwigshafener Haus des Jugendrechts ein Modellprojekt für das ganze Land darstellt und demnächst in Mainz eine vergleichbare Einrichtung geschaffen werden soll (vgl. die LT-Drs. 15/1316 v. 17.7.2007), kommt der in Ludwigshafen bestehenden Situation eine besondere Bedeutung zu.

7.3 Zivilrecht

7.3.1 Das automatisierte Grundbuch – SolumSTAR/SolumWEB

7.3.1.1 Das automatisierte Grundbuchabrufverfahren

Im 20. Tb. (Tz. 7.2.1) hatte der LfD bereits die Einführung des automatisierten Abrufverfahrens beim Grundbuch SolumSTAR/SolumWEB dargestellt. Der LfD hatte sich in diesem Zusammenhang für eine Beschränkung der Abrufberechtigung für Gemeinden auf das Gemeindegebiet, gegen die landesweite Abrufmöglichkeit für Notare und eine Protokollierung der Abrufe dergestalt eingesetzt, dass nicht nur die abfragende Stelle, sondern auch der einzelne Bedienstete, der den Abruf vorgenommen hat, erkennbar ist. Dies erst ermöglicht es, die in § 83 Abs. 1 Satz 3 Grundbuchverordnung vorgesehenen Stichprobenkontrollen durch die aufsichtsführenden Stellen sinnvoll durchzuführen.

Diese Beschränkung der Zugriffsberechtigung insbesondere der Gemeinden haben die Datenschutzbeauftragten des Bundes und der Länder mit einem Schreiben an die Vorsitzende der Justizministerkonferenz gefordert. Leider wurden in der Antwort auf dieses Schreiben nur die bekannten Gegenargumente wiederholt; eine Bewegung in der Sache hin zu einer effizienten technischen Absicherung des Datenschutzes im Bereich des automatisierten Grundbuchabrufverfahrens ist nicht festzustellen.

7.3.1.2 Auskunft aus dem Grundbuch an Miteigentümer

Wiederholt wurden an den LfD Eingaben gerichtet, in denen gerügt wurde, dass andere Personen in den von diesen beantragten Grundbuchauszügen detaillierte Informationen über die bestehenden Grundschulden der Beschwerdeführer und die Bankinstitute, für die diese Grundschulden eingetragen waren, erhalten hätten.

Diesen Eingaben lag regelmäßig die Fallgestaltung zugrunde, dass die Empfänger der Grundbuchkopien und die Beschwerdeführer als Miteigentümer an einem Grundstück miteinander verbunden waren. Dies war den Betroffenen häufig nicht bewusst: So kann diese Fallgestaltung eintreten, wenn Grundbuchgeschäfte vor der Trennung von Grundstücken zu dinglichen Veränderungen führen. Häufig war es so, dass in Wohnanlagen – etwa von Reihenhäusern – an bestimmten Flächen (Wegen, Parkplätzen o.ä.) Gemeinschaftseigentum aller Nachbarn bestand. Diese rechtliche Eigentümergemeinschaft führt zu der grundbuchrechtlich zwangsläufigen Folge, dass bei einem Antrag auf Erteilung eines Grundbuchauszugs jeder Miteigentümer über die Daten aller Mitbetroffenen informiert wird. Der LfD konnte in diesen Fällen nicht weiterhelfen.

7.3.1.3 Die Versendung vollständiger Bestandsverzeichnisse aus dem Grundbuch an Grundstückskäufer

Aufgrund von Eingaben wurde bekannt, dass zumindest in einem Landgerichtsbezirk über einen gewissen Zeitraum hinweg jeder Mitteilung über ein Grundstücksgeschäft das vollständige Bestandsverzeichnis des betroffenen Grundbuchblattes beigefügt war. Dies war deshalb aus Datenschutzsicht höchst bedenklich, da nach der im Land üblichen Gestaltung des Grundbuchs alle im Grundbuchbezirk liegenden Grundstücke eines Eigentümers auf einem einzigen Grundbuchblatt verzeichnet sind; dies kann bei begüterten Landwirten beispielsweise ein umfangreiches Verzeichnis sein. Der Käufer nur eines – vielleicht auch nur kleinen – Grundstücks dieses Landwirts erhielt mit der Unterrichtung über die Eintragung der ihn betreffenden Auflassung eine Liste aller Grundstücke, die der Verkäufer außerdem noch in dem Grundbuchbezirk besitzt.

Nach der Auskunft der Notare, die die jeweiligen ihnen vom Grundbuchamt überlassenen Grundbuchausdrucke an die Parteien des Grundstücksgeschäfts versandten, lag dem eine unzureichende Gestaltung des automatisierten Grundbuchverfahrens zugrunde. Dieses sei aber inzwischen geändert worden. Der LfD hat das Justizministerium um Mitteilung gebeten, ob dieser Vortrag zutrifft, wie lange und ob diese Unzuträglichkeit landesweit bestanden hat sowie, ob nunmehr dieses Problem tatsächlich landesweit gelöst sei.

Derzeit ist die Angelegenheit noch nicht abgeschlossen.

7.3.2 Elektronische Insolvenzbekanntmachungen

Nicht nur nach dem zum 1.1.2007 in Kraft getretenen Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister, sondern auch im Insolvenzrecht sind elektronische Bekanntmachungen die Standardform von Veröffentlichungen. Das Gesetz zur Vereinfachung des Insolvenzverfahrens (BR-Drs. 549/06) sieht als Regelfall nur noch die bislang fakultativ mögliche (§ 9 Abs. 1 Satz 1 InsO) elektronische Bekanntmachung im Internet vor. Sämtliche Insolvenzbekanntmachungen sollen auf einer bundeseinheitlichen Internetplattform veröffentlicht werden und auf diese Weise die Bekanntmachungskosten senken und die Recherchemöglichkeiten verbessern. Auf der anderen Seite aber greift diese Veröffentlichungsform in neuer Weise in die Persönlichkeitsrechte der betroffenen Insolvenzschuldner ein, da die Daten nun weltweit von jedermann abgerufen werden können. Zudem besteht die Gefahr, dass die Daten auch dann noch im Internet gefunden werden können, wenn sie von der eingebenden Stelle längst gelöscht wurden, da Originalseiten auf anderen Internetservern gespiegelt werden (zur Cache-Problematik s. auch Tz. 21.2.5). Datenschutzvorkehrungen sind deshalb von großer Bedeutung. Bisher galten hier die Regelungen der Rechtsverordnung vom 12.2.2002 (BGBl. I S. 677), die gem. § 9 Abs. 2 Satz 3 InsO vom BMJ erlassen worden sind. Diese Verordnung enthält insbesondere Löschungsfristen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben, jederzeit ihrem Ursprung nach zugeordnet und nach dem Stand der Technik durch Dritte nicht kopiert werden können. Mit Wirkung zum 1.1.2007 ist allerdings die bisher in § 9 Abs. 2 Satz 3 Nr. 3 InsO enthaltene Kopierschutzregelung entfallen (Art. 12 Abs. 2 EHUG), weil sie nach dem gegenwärtigen Stand der Technik weitgehend leer laufe. Aus der Sicht des LfD sollte demgegenüber im Interesse der Persönlichkeitsrechte der Betroffenen gesetzlich (in der InsO) ausdrücklich klargestellt werden, dass die Verbreitung der Insolvenzdaten durch Dritte im Internet – insbesondere nach Löschung der Veröffentlichung im amtlichen Informationssystem – verboten ist. Auch wenn ein hundertprozentiger Kopierschutz technisch tatsächlich nicht möglich ist, so sollte doch das technisch machbare Schutzniveau vorgeschrieben werden. Mit den Datenschutzbeauftragten des Bundes und der Länder stimmt der LfD darin überein, dass zumindest über technische und rechtliche Alternativen zu der entfallenen Anforderung des technischen Kopierschutzes nachgedacht werden muss. Es muss wirkungsvoll verhindert werden, dass amtlich bekannt gemachte personenbezogene Daten missbräuchlich genutzt werden. Hierbei handelt es sich angesichts der breiten Nutzung des Internets für öffentliche Bekanntmachungen um ein grundsätzliches datenschutzrechtliches Problem. Technisch könnten vielleicht Verfahren genutzt werden, durch die kommerzielle Urheberrechte geschützt werden sollen. Rechtlich könnte an die Schaffung von Straf- bzw. Bußgeldvorschriften gedacht werden. Darüber hinaus ist daran zu denken, die bestehenden zivilrechtlichen Unterlassungs- und Schadensersatzansprüche effektiver zu gestalten, damit sie auch in diesem Zusammenhang Wirkung entfalten. Dieses Ziel wird von den Datenschutzbeauftragten gemeinsam weiter verfolgt, bislang allerdings erfolglos.

7.4 Justizvollzug

Eine Vielzahl von Eingaben betraf den Bereich der Justizvollzugsanstalten. So wurde die Frage der Information von – dem Anstaltskaufmann helfenden – Mitgefangenen über den Anstaltseinkauf und das verfügbare Guthaben erneut problematisiert und einer – wie jedenfalls derzeit zu hoffen ist – datenschutzverträglichen Lösung zugeführt. Die Bemühungen des Ministeriums der Justiz in diesem faktisch komplexen Zusammenhang verdienen aus der Sicht des LfD besondere Anerkennung.

Die Übermittlung und Nutzung von Gesundheitsdaten innerhalb einer Justizvollzugsanstalt war Gegenstand einer Eingabe, die allerdings zu keinen Änderungen in der Praxis Anlass gab.

Im Zusammenhang mit der Telefonnutzung gab es verschiedene Eingaben, die den Schutz von Verteidigertelefonaten, aber auch die akustische Abschirmung von auf den Fluren installierten Telefonen betraf. Die Justizvollzugsanstalten waren hier grundsätzlich bereit, dem Anliegen des Datenschutzes Rechnung zu tragen.

Immer wieder wurde auch gerügt, dass bei gläsernen Büros innerhalb der Anstalten eine Einsichtnahme auf unterschiedliche Gefangenendaten von außen möglich sei. Hier wurden durch die Justizvollzugsanstalten Gegenmaßnahmen zugesagt.

Besonders bedeutsam aus der Sicht des LfD waren Fragen, die die Verarbeitung von Besucherdaten zum Gegenstand hatten. Immerhin leisten die Besucher einen wichtigen Beitrag im Rahmen der Resozialisierung. Es besteht kein Anlass, sie in ihrem Datenschutzgrundrecht mehr als unbedingt nötig einzuschränken. So ist auch die Sicht des Gesetzgebers, der bezüglich der Besucher strikt auf den Erforderlichkeitsgrundsatz abstellt: Ihre Daten dürfen nur verarbeitet werden, soweit es für Strafvollzugszwecke erforderlich ist. Dem trägt die Praxis aus der Sicht des LfD noch nicht genügend Rechnung. Insoweit besteht noch Diskussionsbedarf mit dem Ministerium der Justiz. Die Überwachung der Besucher während des Besuchs mittels Videokameras, auf die die Besucher hingewiesen worden sind, entspricht dagegen aus der Sicht des LfD der Rechtslage.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 Vorbemerkungen

Die Zahl von gut 1.800 Schulen in Rheinland-Pfalz bringt es mit sich, dass der LfD regelmäßig mit sich wiederholenden Fragestellungen befasst wird. Die Anfragen z.B. zur Internet-Nutzung in der Schule können teilweise mit einem Hinweis auf die bereits bestehenden, im Internet abrufbaren Angebote des LfD erledigt werden. Auf der Homepage des LfD stehen in diesem Zusammenhang beispielsweise unter den Stichworten „Besondere Erläuterungen für den schulischen Datenschutzbeauftragten“ oder „Auswertung der Tätigkeitsberichte“ umfangreiche Informationen zur Verfügung.

Mit einem Vorfall, der auf ein breites Interesse in der Öffentlichkeit gestoßen ist, konnte sich der LfD allerdings nicht beschäftigen. Ein Schüler hatte Teile einer Unterrichtsstunde und insbesondere Äußerungen der Lehrkraft auf seinem Mobiltelefon mitgeschnitten und anschließend einem Rundfunksender zur Verfügung gestellt. Hier konnte der LfD einerseits deshalb nicht tätig werden, weil sich die Schule, an der sich die Angelegenheit ereignete, in kirchlicher Trägerschaft befindet. Das Landesdatenschutzgesetz gilt jedoch nicht unmittelbar für die öffentlich-rechtlichen Religionsgesellschaften. Die beiden großen Religionsgesellschaften haben aber eigene datenschutzrechtliche Regelungen erlassen und Datenschutzbeauftragte bestellt. Andererseits hat der Schüler hier als Privatperson gehandelt, hinsichtlich der dem LfD die Kontrollbefugnis fehlt.

8.1.2 Schule und Datenschutz

Dieses Thema wird in den nächsten Jahren ein Arbeitsschwerpunkt des LfD sein. Denn es verfestigt sich der Eindruck, dass die Jugendlichen und überhaupt die jüngere Generation dem Schutz ihrer Daten keine besondere Bedeutung beimessen und insbesondere über das Internet leichtfertig persönliche Daten verbreiten. Eine Umfrage hat laut dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) ergeben, dass die Hälfte der 14- bis 29-Jährigen private Daten im Internet veröffentlicht.

Der LfD möchte einen Beitrag dazu leisten, das Datenschutzbewusstsein der Schüler zu fördern. Denn die einmal in die Speicher der Suchmaschinen gelangten Daten sind nur schwer zu löschen und auch Jahre danach noch abrufbar. Es ist nicht

auszuschließen, dass sich daraus Nachteile z.B. für Bewerbungen ergeben können. Aus der Sicht des LfD muss den Jugendlichen vermittelt werden, dass sie auch selbst für die Wahrung ihrer Privatsphäre zu achten haben.

Erste Aktivitäten wurden im Berichtszeitraum bereits auf den Weg gebracht. So wurde eine Mitarbeit beim Programm „Medienkompetenz macht Schule“ der Landesregierung vereinbart. Als Termin für eine diese Kooperation zum Ausdruck bringende Auftaktveranstaltung ist der Europäische Datenschutztag am 28.1.2008 vorgesehen. Diese Verbindung bietet sich deshalb an, weil der Europarat mit dem Europäischen Datenschutztag das Bewusstsein für den Datenschutz bei den Bürgern stärken möchte. Die Veranstaltung wird insbesondere an die behördlichen Datenschutzbeauftragten der Schulen gerichtet sein. Damit verbunden werden soll der Aufbau eines Netzwerkes der schulischen Datenschutzbeauftragten.

Weiterhin hat der LfD angeregt, auf der Herbstkonferenz 2007 der Datenschutzbeauftragten des Bundes und der Länder die Einrichtung einer Arbeitsgruppe „ Datenschutz und Schule“ zu beschließen. Diese Arbeitsgruppe soll vor allem einen Beitrag zur Verbesserung des Datenschutzbewusstseins bei Schülern leisten.

8.1.3 Bildungsberichterstattung und Schulstatistik

Bestrebungen der Kultusministerkonferenz, eine einheitliche und bundesweite Datenbank zu schaffen, mit der Bildungsverläufe von Schülern nachvollziehbar sein sollen, waren Anlass für eine intensive Auseinandersetzung des LfD sowie seiner Kollegen in den Ländern mit diesem Thema. In diesem Zusammenhang hat die Kultusministerkonferenz die Einführung des sog. Kerndatensatzes, der länderübergreifend übereinstimmende Inhalte der zu erhebenden Merkmale (Individualdaten) festlegt, beschlossen. Jeder Schüler soll über die Vergabe einer Identifikationsnummer möglichst für den gesamten Bildungsverlauf nur mit einem Datensatz geführt werden. Als Begründung wurde genannt, dass eine solche Datei unter „Nutzung von Individualdaten als Instrument der Koordinierung politischer und planerischer Maßnahmen sowie für die internationale Zusammenarbeit“ notwendig sei.

Die Datenschutzbeauftragten sehen eine solche Totalerhebung, wenn die Datenverarbeitung personenbeziehbar erfolgt, sehr kritisch. Nach den verfassungsrechtlichen Vorgaben ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen, wie z.B. einer Stichprobe (wie PISA), für die Betroffenen erreicht werden kann. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 26./27.10.2006 (vgl. Anlage 17) hingewiesen.

Mittlerweile verzichtet die Kultusministerkonferenz darauf, eine zentrale länderübergreifende Datenbank zu betreiben. Statt dessen soll ein technisch und datenschutzrechtlich möglicher Weg aufgezeigt werden, um künftig die statistische Betrachtung von Schülerbiografien zu ermöglichen (Hash-Codierung). Dabei soll sichergestellt werden, dass für alle Auswertungen das Statistikgesetz gilt. Die Hash-Nummer (Fallnummer) soll über die Jahre konstant bleiben und statistische Aussagen über Bildungsverläufe ermöglichen. Die zur Erzeugung der Hash-Nummer notwendigen personenbezogenen Merkmale werden nach der Berechnung der Nummer aus dem Datensatz vollständig gelöscht, sodass aus der Sicht der Kultusministerkonferenz ein Rückbezug auf eine bestimmte Person nahezu ausgeschlossen sein soll.

Aber auch während eines Gesprächs zwischen Mitgliedern der Kommission für Statistik der Kultusministerkonferenz und Vertretern der Konferenz der Datenschutzbeauftragten im August 2007 konnten nicht alle aus datenschutzrechtlicher Sicht relevanten Punkte geklärt werden. Insbesondere die vorgesehene Totalerhebung zur Durchführung von Bildungsverlaufsuntersuchungen wird unverändert kritisch gesehen, soweit individualisierbare Daten verarbeitet werden sollen. Die Datenschutzbeauftragten des Bundes und der Länder werden daher die weitere Entwicklung aufmerksam beobachten und kritisch begleiten.

In Rheinland-Pfalz ist für die Statistik im Schulbereich die Umstellung von zusammengefassten Daten (Summenbeträge) auf Individualdaten bereits erfolgt. Rechtsgrundlage hierfür ist § 67 Abs. 8 SchulG. Danach sind die Schulen für die Statistik im Schulbereich verpflichtet, den Schulbehörden, den Schulträgern und dem Statistischen Landesamt die erforderlichen Einzelangaben der Schüler, Lehrkräfte, pädagogischen und technischen Fachkräfte sowie des sonstigen pädagogischen Personals zu übermitteln. Der Name, der Tag der Geburt, die Adresse und die Personalnummer der Betroffenen – also personenbezogene Daten – dürfen aber an das Statistische Landesamt und die Schulträger nicht übermittelt werden. Außerdem werden die Datensätze derzeit lediglich mit einer laufenden Nummer versehen, die von Jahr zu Jahr unterschiedlich ist. Die Darstellung von Bildungsverläufen ist somit nicht möglich, da die Datensätze aus verschiedenen Jahren nicht miteinander verknüpft werden können. Die Umstellung auf den Kerndatensatz ist bereits im Gang.

Zwischen dem MBWJK und dem LfD besteht Einigkeit darüber, dass im Falle der Umsetzung des derzeitigen Konzepts der Kultusministerkonferenz gerade wegen der Vergabe einer dauerhaften Fallnummer die vorhandenen gesetzlichen Regelungen geprüft und ggf. entsprechend geändert werden müssen.

8.1.4 Agentur für Qualitätssicherung, Evaluation und Selbständigkeit von Schulen – AQS

Aufgabe der AQS ist die Unterstützung der Schulen in ihrer Qualitätsarbeit. Sie führt die externe Evaluation – eine Säule der Qualitätsentwicklung – an den rund 1.600 rheinland-pfälzischen Schulen durch. Wie die AQS betont, wird die externe Evaluation national und international als bedeutendes Element der Qualitätssicherung im Bildungsbereich angesehen. Die externe Evaluation hat das Ziel, der einzelnen Schule Rückmeldungen zum aktuellen Stand der eigenen Qualitätsentwicklung zu geben. Die Berichte bilden die Basis für Zielvereinbarungen zwischen Schule und Schulaufsicht. Die AQS ist eine eigenständige Organisationseinheit im Geschäftsbereich des MBWJK und ist dem Präsidenten der ADD unterstellt.

Vom MBWJK wurde der LfD bereits im Rahmen des Aufbaues der Behörde wegen des verwendeten Onlinebewerbungsverfahrens eingebunden. Auch hinsichtlich des Starts der Testphase, die der Entwicklung und Erprobung der Methoden und Verfahren zur Evaluation diente, mit rund 50 Pilotschulen Ende 2006 ist der LfD beratend hinzugezogen worden.

Aus datenschutzrechtlicher Sicht ist es zwar erklärtes Ziel der AQS, so wenig personenbezogene Daten wie möglich zu erheben. Allerdings befragen die Schulteams Schüler, Eltern und Lehrkräfte, beobachten Lehr- und Lernsituationen und führen Schulbegehungen durch. Rechtsgrundlage für die Datenerhebung ist § 67 Abs. 2 SchulG. Danach können die Schulbehörden zu Zwecken der Evaluation von Schulen geeignete Verfahren einsetzen und durch Befragungen und Unterrichtsbeobachtungen erhobene Daten verarbeiten. Die Betroffenen werden vorab über das Ziel des Vorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung ihrer Daten informiert. Personenbezogene Daten für die Evaluation von Schule dürfen ohne Einwilligung der Betroffenen verarbeitet werden, wenn das öffentliche Interesse an der Durchführung eines von der obersten Schulbehörde genehmigten Vorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann. Sind diese Kriterien nicht erfüllt, können personenbezogene Daten nur mit Einwilligung der Betroffenen erhoben werden.

Die datenschutzrechtliche Beurteilung anhand der bisher bekannten Angaben zur Vorgehensweise hat ergeben, dass mit den vorgelegten Fragebögen eine faktisch anonyme Datenerhebung hinsichtlich der Schüler sowie der Eltern bzw. Erziehungsberechtigten erfolgt. Faktisch anonym bedeutet, dass Einzelangaben über persönliche oder sachliche Verhältnisse nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die Beurteilung der Frage, ob Daten faktisch anonymisiert oder personenbeziehbar sind, erfordert eine Risikoabwägung, bei der die Sensibilität der Daten und die rechtlich zulässigen Identifizierungsmöglichkeiten sowie das Identifizierungsinteresse zu berücksichtigen sind. Maßgeblich ist hier einerseits die niedrige Sensibilität der zu erhebenden Daten. Andererseits müssten sich zur Beschaffung von zur Identifizierung von Einzelpersonen notwendigem Zusatzwissen Lehrkräfte und Mitarbeiter der AQS pflichtwidrig verhalten. Für die Befragung ist somit keine Einwilligung notwendig.

Eine Prüfung der praktischen Arbeit der Mitarbeiter der AQS ist seitens des LfD noch nicht erfolgt. Nachdem die externe Evaluation mit Beginn des Schuljahres 2007/2008 in das Standardverfahren übergegangen ist, wird dieses demnächst Gegenstand örtlicher Feststellungen sein.

8.1.5 Abstammungserklärungen in der Schülerakte

Im Rahmen örtlicher Feststellungen bei verschiedenen rheinland-pfälzischen Schulen hat der LfD Kopien von Abstammungsurkunden in den Schülerakten gefunden. Die Schulen erklärten hierzu, die Vorlage von Abstammungserklärungen dienten dazu, die genaue Schreibweise der Schülernamen festzustellen. Aus den Abstammungserklärungen ergibt sich jedoch nicht nur die Schreibweise der Namen. Darin können vielmehr auch Angaben zur Religionszugehörigkeit der Eltern enthalten sein. Datenschutzrechtlich ist es allenfalls zulässig, die Eltern um Vorlage der Abstammungserklärung mit dem Hinweis zu bitten, dass die Vorlage freiwillig ist und alle anderen Daten außer dem Namen abgedeckt werden können. Eine Aufnahme in die Schülerakte ist nicht erforderlich und damit unzulässig. Das zuständige Ministerium teilte diese Auffassung und bat die Schulbehörde, auf eine diesen Grundsätzen entsprechende einheitliche Praxis in den Schulen hinzuwerfen.

8.1.6 Muttersprachlicher Unterricht und Leistungsbeurteilungen durch den Ausländerbeirat

Schüler, deren Muttersprache und Herkunftssprache nicht Deutsch ist, können Unterricht in ihrer Mutter- oder Herkunftssprache erhalten. Dies soll die schulische und soziale Integration unterstützen und die sprachliche und kulturelle Persönlichkeitsbildung fördern. Dieser Unterricht ist ein zusätzliches Angebot, die Teilnahme ist freiwillig. Lehrkräfte für diesen Unterricht müssen eine nachgewiesene Lehramtsbefähigung ihres Heimatlandes oder Deutschlands, Unterrichtserfahrung im Sprachunterricht und ausreichende deutsche Sprachkenntnisse haben. Über die Einrichtung und Organisation entscheidet die Schulbehörde. Die Lehrkräfte sollen von der Schulbehörde einer Stammschule zugewiesen werden. An dieser Stammschule sind sie Teil des Kollegiums mit allen Rechten und Pflichten. Die Leistungsbeurteilung der Schüler in diesem Unterricht wird in der,

der Klassenstufe entsprechenden Form in das Zeugnis aufgenommen. Auf Wunsch der Eltern kann statt dessen eine gesonderte Bescheinigung ausgestellt werden.

Ein Ausländerbeirat organisierte auf Wunsch der Schulbehörde und der Eltern den muttersprachlichen Unterricht für eine Stadt. Als der Ausländerbeirat die Leistungsbeurteilungen auf seinem eigenen Briefkopf an die jeweiligen Schulen übermittelte, kam es zu Irritationen bei den betroffenen Eltern. Das Vorgehen des Ausländerbeirates war sicherlich dazu geeignet, den Eindruck zu erwecken, er selbst trage die Verantwortung für den muttersprachlichen Unterricht und nehme Benotungen bzw. Leistungsbeurteilungen vor. Dies war nicht im Sinne des Gesetzgebers, der für die Benotung das reguläre schulische Verfahren vorgesehen hat. Der Ausländerbeirat hat hierdurch unzulässiger Weise Kenntnis von personenbezogenen Informationen der einzelnen Schüler erhalten. Diese sollten nur dem Lehrer des muttersprachlichen Unterrichts bzw. der Stammschule vorliegen. Diese Einsicht setzte sich auch bei der Schulbehörde und beim Ausländerbeirat durch: die Unterrichtsorganisation wurde geändert. Die Lehrer sind jetzt Stammschulen zugeordnet und der Ausländerbeirat hat mit dem Unterricht nichts mehr zu tun.

8.1.7 Sind Läuse so schlimm wie Typhus und Cholera?

Fälle von Verlausung sind von den Schulen genauso an das Gesundheitsamt zu melden wie z.B. das Auftreten von Typhus oder Cholera. Ein Vater fand dies unverhältnismäßig und wandte sich daher an den LfD.

Sorgeberechtigte für ein Kind sind gem. § 34 Abs. 5 IfSG verpflichtet, die Schule zu informieren, wenn ihr Kind von Läusen befallen ist. Die Schulleitung wiederum ist gem. § 34 Abs. 6 IfSG verpflichtet, unverzüglich das zuständige Gesundheitsamt zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen. Der Gesetzgeber hat neben anderen schweren Erkrankungen auch den Fall der Verlausung in die Informationspflicht aufgenommen. Denn Kopfläuse können von Mensch zu Mensch übertragen werden und stellen eine deutliche Beeinträchtigung des Wohlbefindens dar. Auch wenn sie praktisch keine Krankheitserreger übertragen, werden sie in einigen Bereichen bestimmten übertragbaren Krankheiten gleichgestellt.

Die Übermittlung personenbezogener Daten an das Gesundheitsamt greift in das Persönlichkeitsrecht der Betroffenen ein. Dieses wird jedoch nicht schrankenlos gewährt, sondern kann durch Gesetz eingeschränkt werden. Das hat der Gesetzgeber durch die Meldeverpflichtung im IfSG getan. Die Einschränkung beruht auf einer wirksamen Rechtsgrundlage. Durch die Meldeverpflichtung sollen andere Schulbesucher in ihrem Recht auf körperliche Unversehrtheit geschützt werden. Der Gesetzgeber hat hier also zwei bestehende Grundrechte gegeneinander abgewogen. Die getroffenen Bewertungen sind aus datenschutzrechtlicher Sicht nicht als unverhältnismäßig zu bezeichnen. Die §§ 6 ff. IfSG betreffen das Meldewesen bestimmter Krankheiten in allen denkbaren Fällen. Darüber hinaus hat der Gesetzgeber zusätzliche Vorschriften für Schulen und sonstige Gemeinschaftseinrichtungen geschaffen, aufgrund deren Besonderheiten besondere Schutzverpflichtungen des Staates bestehen. Diese gehen den allgemeinen Regelungen vor.

8.1.8 Molekularbiologisches Schulpraktikum im Fach Biologie

Ein Universitätsfachbereich hat in Zusammenarbeit mit verschiedenen Schulen ein Konzept für ein molekularbiologisches Schulpraktikum für Biologieleistungskurse entworfen. Die Schüler sollen an der Universität unter fachlicher Anleitung DNA aus ihrem eigenen Blut isolieren und später analysieren. Die Schulbehörde wandte sich an den LfD mit der Bitte um Beratung bzw. Prüfung.

Im Verlauf der Prüfung war unter anderem der beabsichtigte Umfang der Analysen zu klären. Gegen die Erstellung eines sog. genetischen Fingerabdrucks auf der Grundlage einer vorherigen Einwilligung bestanden grundsätzlich keine durchgreifenden datenschutzrechtlichen Bedenken. Anders hätte es sich verhalten, wenn darüber hinausgehend DNA-Analysen beabsichtigt gewesen wären, die Rückschlüsse z.B. auf evtl. Krankheiten und somit über persönlichkeitsrelevante Erbinformationen zugelassen hätten. Insoweit wäre es fraglich gewesen, ob Lehrkräfte oder auch Mitschüler auf der Grundlage einer Einwilligung von Gendefekten und daraus resultierenden Krankheitsveranlagungen einer anderen Person hätten Kenntnis erhalten dürfen. Da zum Grundrecht auf informationelle Selbstbestimmung auch das Recht auf Nichtwissen gehört, wären bei einer solch weitgehenden Analyse der Proben die Schüler im Rahmen der durchzuführenden Information auch auf mögliche physische oder psychische Folgen der Kenntnisnahme von einem entsprechenden Untersuchungsergebnis für sich sowie ihre Familie hinzuweisen gewesen. Eine solch weitgehende Analyse war aber zu keinem Zeitpunkt beabsichtigt.

Nachdem der LfD weiterhin problematisiert hatte, dass eine DNA-Probe an sich niemals absolut anonym erhoben und somit unter Umständen aufgrund evtl. vorhandener Referenzproben immer einer bestimmten Person zugeordnet werden kann, wurde seitens der Universität auch die Absicht aufgegeben, die Schüler darum zu bitten, dass ihre DNA-Proben über das Schulpraktikum hinaus der Forschung zur Verfügung gestellt werden. Denn eine Einwilligung kann grundsätzlich nur gegenüber einem konkret benannten Forschungsvorhaben wirksam erklärt werden.

8.2 Wissenschaft und Hochschulen

8.2.1 Befragungen in Schulen

Die überwiegende Zahl der durch den LfD zu bewertenden Befragungen im Rahmen von wissenschaftlichen Forschungsarbeiten finden aufgrund des dort vorhandenen vielfältigen Personenkreises nach wie vor an Schulen statt. So wurden dem LfD beispielsweise Befragungen zu folgenden Themen vorgelegt:

- Weibliche Identität – ein Produkt medienspezifischer Marketingstrategien
- Ernährungsbewusstsein im Schulalltag
- Schwimmfähigkeit von Schüler/Innen an allgemeinbildenden Schulen
- Lehr- und Lernbarkeit von englischen Präpositionen
- Jugend und Europa
- Projekt Respekt – Befragung zum Thema Gewalt und Gewaltprävention
- Leistungsmotivation von Individualsportlern im Nachwuchsleistungssport

Neue Streitgegenstände sind zu den im letzten Tb. unter Tz. 8.1.2 dargestellten Gesichtspunkten nicht hinzugekommen. In aller Regel werden die Hinweise, Anregungen und Bedenken des LfD – wie dies auch im Genehmigungsbescheid der Schulbehörde gemäß § 67 Abs. 6 SchulG vorgesehen ist – von den Verantwortlichen der Forschungsarbeiten berücksichtigt bzw. umgesetzt. Eine unrühmliche Ausnahme bildet ein außerhalb von Rheinland-Pfalz ansässiges Forschungsinstitut, das eine bundesweite Studie durchführte, in deren Rahmen mehrere zehntausend Schüler sowie auch Lehrkräfte zu heiklen Themen befragt wurden.

Mit den dem LfD zur Prüfung vorgelegten Fragebögen wurden den Schülern der 4. Klasse beispielsweise folgende Fragen gestellt:

Wenn Eltern richtig wütend sind, kommt es vor, dass sie ihre Kinder schlagen. Wie oft ist dir das in den letzten 4 Wochen passiert? Meine Mutter/mein Vater hat

- .....
- *mir eine runtergehauen.*
- *mich mit der Faust geschlagen oder mich getreten.*
- *mich geprügelt bzw. mich zusammengeschlagen.*

Hast du schon jemals folgende Dinge getan? Wenn ja, dann gib bitte an, wie häufig in den letzten Monaten:

- .....
- *Einem anderen Kind gedroht, damit es mir etwas gibt.*
- *In einem Kaufhaus oder Geschäft etwas gestohlen.*
- *Absichtlich Fenster, ... oder ähnliche Dinge beschädigt.*
- .....
- *Gezündelt oder etwas in Brand gesteckt.*

Der Fragebogen für die Schüler der 9. Klasse enthielt z.B. folgende Fragen:

Wie ist deine Meinung zu folgenden Aussagen über deine Freundesgruppe?

- .....
- .....
- *Wir handeln mit Drogen. Stimmt nicht/kaum/eher/genau*

Viele Menschen haben als Jugendliche auch absichtlich und nicht aus Spaß jemanden verprügelt und verletzt. Hast du schon jemals Folgendes getan?

- .....
- .....
- *Alleine oder mit anderen Personen zusammen jemanden gegen seinen o. ihren Willen unsittlich angefasst oder mit Gewalt oder durch ernsthafte Androhung von Gewalt zu sexuellen Handlungen oder zur Duldung von sexuellen Handlungen gezwungen? Wie alt warst du, als du das zum allerersten Mal getan hast? Wie oft hast du das im Jahr 2006 getan?*

Gemäß § 67 Abs. 6 SchulG bedarf die Verarbeitung von personenbezogenen Daten für wissenschaftliche Untersuchungen in der Schule durch externe Stellen neben der oben bereits erwähnten Genehmigung der Schulbehörde auch der Einwilligung der

Betroffenen. Im Wesentlichen wurde seitens des LfD geltend gemacht, dass mit den zur Prüfung vorgelegten Fragebögen zumindest personenbeziehbare Daten erhoben werden, sodass entgegen entsprechender Hinweise des Instituts in Informationsschreiben an die Betroffenen nicht von einer anonymen Befragung ausgegangen werden konnte. Für die Wirksamkeit einer zur Datenerhebung erforderlichen Einwilligung der Betroffenen war deshalb eine ausreichende vorherige Information zu fordern. Nach Ansicht des LfD war der Inhalt der vorgelegten Informationsschreiben jedoch weder für die Befragung der 4. noch 9. Klassen ausreichend. Die Eltern hätten in diesem Zusammenhang grundsätzlich darauf hingewiesen werden müssen, dass die Schüler u.a. auch zu Gewalterfahrungen in Familie – also unmittelbar zu ihren Eltern – und Schule sowie dazu befragt werden, ob sie sich bereits abweichend verhalten (z.B. Diebstahl, Schulschwänzen) haben. Deshalb war für den LfD auch hinsichtlich der Befragung der 9. Klassen eine ausdrückliche Einwilligung der Eltern erforderlich. Die vom Institut angedachte Widerspruchsmöglichkeit für die Eltern der Schüler der 9. Klassen konnte nicht akzeptiert werden, da eine unterbliebene Rückäußerung und somit das „Schweigen“ der Eltern nicht als Zustimmung zur Teilnahme der Schüler an der Befragung gewertet werden kann. Die Datenerhebung wäre dann ohne Rechtsgrundlage erfolgt.

Das Institut hielt dem entgegen, dass eine nähere Information der Eltern bzgl. der Fragen zu Gewalterfahrungen in der Familie gerade dazu führen werde, dass „prügelnde Eltern ihren Kindern die Teilnahme verweigern“. Dies gelte auch für die Familien der Kinder, die häufiger verbotene Dinge tun. Schließlich sei bei einem Festhalten an einer ausdrücklichen Einwilligung der Eltern damit zu rechnen, dass nach den bisherigen Erfahrungen dann insbesondere Hauptschüler und solche aus sozialen Randlagen überproportional häufig von der Teilnahme an der Studie ausgeschlossen seien. Insgesamt werde dadurch der Aussagewert der Studie gefährdet. Vor diesem Hintergrund war der LfD dazu bereit, in Anbetracht der Wissenschaftsfreiheit zu akzeptieren, dass gegenüber den Eltern die Inhalte der Fragebögen bzw. der Forschung nur in Grundzügen beschrieben werden. Als Ausgleich dazu sollte den Eltern die Möglichkeit eingeräumt werden, im Vorfeld der Befragung im Schulsekretariat Einblick in den Schülerfragebogen nehmen zu können.

Oben genannte und weitere mit der geplanten Studie zusammenhängende datenschutzrechtliche Bedenken wurden auch von anderen Landesbeauftragten vertreten. Aufgrund dessen wurde die Angelegenheit von Vertretern der Kultusministerkonferenz sowie der Datenschutzbeauftragten mit dem Forschungsinstitut erörtert. Als Lösung verständigte man sich darauf, dass bei der Befragung ausschließlich anonyme Daten erhoben und die Fragebögen sowie das Verfahren entsprechend geändert werden. Die Erteilung einer Einwilligung durch die Betroffenen wäre somit nicht mehr erforderlich gewesen. Für den Fall, dass die Befragungen an Schulen mit den beanstandeten Fragebögen bereits begonnen oder sogar schon abgeschlossen waren, wurde dem Forschungsinstitut seitens eines Datenschutzbeauftragten insoweit entgegengekommen, dass die Fragebögen nicht vernichtet werden mussten. Allerdings wurde die Forderung gestellt, dass die Fragebögen nur insoweit elektronisch erfasst und ausgewertet werden dürfen, als die Informationen zulässigerweise hätten erhoben werden dürfen.

Im weiteren Verlauf der Angelegenheit stellte sich dann heraus, dass die Befragungen an den rheinland-pfälzischen Schulen unter Verwendung der unveränderten Fragebögen bereits abgeschlossen wurden, ohne die geäußerten datenschutzrechtlichen Bedenken auszuräumen. Der LfD hat gegenüber dem Forschungsinstitut geltend gemacht, dass diese Vorgehensweise im Widerspruch zum Genehmigungsbescheid der Schulbehörde steht und aus datenschutzrechtlicher Sicht nicht vertretbar ist. Gleichzeitig wurde das Institut zu einer ausdrücklichen Bestätigung aufgefordert, dass entsprechend der oben geschilderten Absprache vorgegangen wird und alle in unzulässiger Weise erhobenen Daten nach dem Erfassen der Fragebögen aus den Datensätzen gelöscht werden.

Weiterhin wurde, um vergleichbare Fälle nach Möglichkeit zu vermeiden, die zukünftige Vorgehensweise mit der Schulbehörde abgestimmt. U.A. wurde der gegenseitige Austausch von Genehmigungsbescheid und datenschutzrechtlicher Stellungnahme vereinbart. Weiterhin wird die Einbindung des LfD künftig im Genehmigungsbescheid als aufschiebende Bedingung formuliert und darauf hingewiesen, dass der Forschende ohne Genehmigung handelt, wenn die Einwände und Anregungen des LfD nicht berücksichtigt werden.

8.2.2 Einführung eines flächendeckenden Mammographie-Screening-Programms und Mitwirkung des Landeskrebsregisters

Der Deutsche Bundestag hat 2002 die Einführung eines qualitätsgesicherten, bundesweiten und bevölkerungsbezogenen Mammographie-Screening-Programms beschlossen und mit der Einführung den Bundesausschuss der Ärzte und Krankenkassen beauftragt. Ein Beschluss des Bundesausschusses zur entsprechenden Änderung der Richtlinien über die Früherkennung von Krebserkrankungen sowie die Vorschriften der Röntgenverordnung ist die Basis für die bundesweite Einführung eines Mammographie-Screenings. In diesem Rahmen soll jede Frau zwischen ihrem fünfzigsten bis zur Vollendung des siebzigsten Lebensjahres alle zwei Jahre schriftlich zu einer Untersuchung auf freiwilliger Basis eingeladen werden. Dieses Angebot richtet sich insbesondere an gesetzlich versicherte Patientinnen, da die Kosten für ein Mammographie-Screening von den gesetzlichen Krankenkassen bisher nicht erstattet wurden.

Im Hinblick darauf, dass für die Einladungen Daten der Melderegister verwendet werden sollen, hatte der LfD frühzeitig (siehe auch 20. Tb., Tz. 4.4) auf die im Bereich des Melderechts vorhandenen Probleme hingewiesen. Dabei stellte sich für den LfD zunächst die Frage, ob die Meldeämter überhaupt zur Herausgabe dieser Daten befugt sind, zumal die Datenweitergabe auch die privat versicherten Frauen betrifft, die das Angebot des Mammographie-Screenings ggf. nicht in Anspruch nehmen möchten.

Wegen dieser Bedenken wurde in § 20 MeldDÜVO die Datenübermittlung für Zwecke der Durchführung des Programms zur Früherkennung von Brustkrebs durch Mammographie-Screening geregelt. Für die Versendung der Einladungen ist die sog. Zentrale Stelle, deren Einrichtung in Rheinland-Pfalz von der Kassenärztlichen Vereinigung übernommen wurde, zuständig. Zur Erfüllung ihrer Aufgaben bekommt die Zentrale Stelle regelmäßig folgende Daten des o.g. Personenkreises durch die Meldebehörden übermittelt:

- Vor- und Familienname,
- frühere Namen,
- Doktorgrad,
- Geburtstag und -ort
- gegenwärtige Anschrift.

Die Zentrale Stelle bildet aus diesen Daten eine Teilnehmernummer sowie nach dem Vorbild des Landeskrebsregisters eine Kontrollnummer. Außerdem erstellt die Zentrale Stelle aus Vor- und Familienname sowie gegenwärtiger Anschrift eine Einladungsliste. Danach werden alle aus den Melderegistern stammenden Daten umgehend gelöscht. Nach Rücklauf der Einladungsliste von der Screening-Einheit, bei der die Untersuchung stattfindet, und Erinnerung der Frauen, die bisher auf die Einladung nicht reagiert haben, löscht die Zentrale Stelle auch die personenbezogenen Daten der Einladungsliste und speichert die Teilnehmernummer, die Kontrollnummer, den vorgeschlagenen oder den wahrgenommenen Termin und den Ort der Untersuchung. Diesbezüglich sind keine datenschutzrechtlichen Einwände zu erheben.

Die Krebsfrüherkennungsrichtlinien fordern auch die Evaluation des Früherkennungsprogramms auf der Basis von anonymisierten und aggregierten Daten. Zur Feststellung von falschnegativen Diagnosen im Mammographie-Screening ist ein regelmäßiger anonymisierter Abgleich mit den Daten der jeweiligen Krebsregister erforderlich. Die oben erwähnte Kontrollnummer wird dafür von der Zentralen Stelle in regelmäßigen Abständen an das zuständige Krebsregister übermittelt und mit den dort gespeicherten Kontrollnummern abgeglichen. Das Krebsregister meldet die Kontrollnummer der gemeldeten Brustkrebsfälle von Frauen, die am Früherkennungsprogramm teilgenommen haben, an die Zentrale Stelle. Das rheinland-pfälzische LKRG ließ einen solchen Abgleich in seiner bisherigen Fassung nicht zu. Daher wurde § 9a in das Gesetz eingefügt, der die Mitwirkung des Krebsregisters nicht nur beim Mammographie-Screening, sondern auch bei anderen Früherkennungsprogrammen regelt. Der LfD wurde frühzeitig beteiligt. Seine Anregungen für eine datenschutzgerechte Ausgestaltung der Regelung sind berücksichtigt worden. Im Fall des Mammographie-Screenings können bereits zum Abgleich die Kontrollnummer, die Teilnehmernummer sowie verschiedene epidemiologische Daten (Geschlecht, Monat und Jahr der Geburt, Wohnort oder Gemeindekennziffer) an die Vertrauensstelle beim Krebsregister übermittelt werden (§ 9a Abs. 1 Satz 2 LKRG). Dies ist nach Auffassung des Krebsregisters notwendig, um möglichen Fehlzuordnungen durch die erzeugten Kontrollnummern im Rahmen einer Plausibilitätskontrolle vorbeugen zu können. Dem Krebsregister ist es auf dieser Basis regelmäßig nicht möglich, einen konkreten Personenbezug herzustellen.

Als weitere Voraussetzung für eine Mitwirkung des Krebsregisters muss eine Genehmigung durch das MASGFF erteilt werden. In diesem Zusammenhang sind Stellungnahmen der Ethikkommission der Landesärztekammer und des LfD einzuholen. Die Anhörung des LfD ist in diesem Zusammenhang mittlerweile erfolgt. Seitens des LfD wurden hinsichtlich der Genehmigung des Antrags des Landeskrebsregisters, soweit es den in § 9a Abs. 1 Satz 2 und Satz 3 LKRG geregelten Datenfluss betrifft, keine Bedenken geäußert.

Das Mammographie-Screening-Programm wird den LfD sowie die Datenschutzbeauftragten des Bundes und der Länder aber auch im kommenden Berichtszeitraum beschäftigen. Denn zum einen wird der LfD das Verfahren zur Durchführung des Mammographie-Screenings im Rahmen örtlicher Feststellungen noch weiter überprüfen. Zum anderen hat die Kooperationsgemeinschaft Mammographie, die zur Koordinierung der Einführung eines flächendeckenden Mammographie-Screening-Programms gegründet wurde, um Zustimmung gebeten, dass teilweise abweichend von den Krebsfrüherkennungsrichtlinien Postleitzahl, Wohnort, Geburtsmonat und Geburtsjahr dauerhaft bei der Zentralen Stelle im Mammographie-Programm gespeichert und von dort im Rahmen des Abgleichs an das jeweilige Krebsregister zur Verbesserung der Übereinstimmungswerte übermittelt werden dürfen. Zusätzlich möchte die Kooperationsgemeinschaft erreichen, dass eine eigens zur Vereinfachung des Abgleichs gebildete Kommunikations-ID verwendet wird.

Weiterhin soll das jeweils zuständige Krebsregister in die Lage versetzt werden, zusammen mit der Kommunikations-ID verschiedene histologische Daten zur korrekten Identifizierung und ersten differenzierten Auswertung der Intervallkarzinome an die Zentrale Stelle übermitteln zu dürfen. Schließlich hält es die Kooperationsgemeinschaft für notwendig, dass Screening-Datum und Ergebnis der letzten Screening-Untersuchung aller an Brustkrebs erkrankten Teilnehmerinnen an das Krebsregister zur Ermöglichung der Mortalitätsevaluation übermittelt werden. Diesbezüglich sieht das Bundesministerium für Gesundheit Klärungsbedarf und die Datenschutzbeauftragten mehrerer Bundesländer haben dagegen Bedenken erhoben. Insbesondere wurde geltend gemacht, dass die zusätzlich gewünschten Datenübermittlungen nur zulässig seien, wenn eine entsprechende Rechtsgrundlage vorliege. In Rheinland-Pfalz ist die Übermittlung histologischer Daten vom Krebsregister an die Zentrale Stelle sowie die Übermittlung bestimmter Daten an das Krebsregister zur Mortalitätsevaluation in § 9a LKRG jedenfalls nicht vorgesehen. Der LfD ist mit anderen Datenschutzbeauftragten der Meinung, dass zunächst der für eine Evaluierung des Mammographie-Screening-Programms erforderliche Datenaustausch fachlich festgestellt werden muss, bevor Lösungswege bzw. die Einzelheiten neuer gesetzlicher Regelungen erörtert werden können.

8.2.3 Aktenzeichen als Sozialdaten?

Im Rahmen eines Forschungsprojekts „Betrug im Gesundheitswesen“ trat eine Universität an die AOK Rheinland-Pfalz mit der Bitte heran, ihr Aktenzeichen von solchen Strafverfahren zu übermitteln, bei denen es sich um Betrugsdelikte im Gesundheitsbereich zum Nachteil der Krankenkasse handelte. Mithilfe dieser Aktenzeichen wollte man Einsicht in die Strafverfahren bei den Staatsanwaltschaften nehmen, um Informationen für das Forschungsprojekt zu sammeln. Eine direkte Anfrage bei der Staatsanwaltschaft wäre nicht sinnvoll gewesen, da diese die Strafverfahren nicht mit der Zielrichtung Betrug im Gesundheitswesen auswerte und so die entsprechenden Aktenzeichen nicht hätte nennen können. Die anfragende Universität war der Ansicht, dass es sich bei den Aktenzeichen nicht um Sozialdaten handelt.

Diese Auffassung wurde vom LfD geteilt. Die Aktenzeichen stellten zunächst kein personenbezogenes oder auch personenbeziehbares Datum dar. Ein Personenbezug konnte von der Universität erst hergestellt werden, wenn sie Einsicht in die Strafakten bei der Staatsanwaltschaft erhalten hätte. Dies setzte einen entsprechenden Antrag voraus, der von der Staatsanwaltschaft auch unter dem Gesichtspunkt des Schutzes personenbezogener Daten zu prüfen gewesen wäre. Die Strafakten bei der Staatsanwaltschaft stellen aber keine Sozialdaten im Sinne von § 35 SGB X dar. Einer Übermittlung der Aktenzeichen für das konkrete Forschungsprojekt standen daher keine datenschutzrechtlichen Gründe entgegen.

8.3 Sonstiges

8.3.1 Häuserchronik einer Ortsgemeinde

Vor dem Druck einer Ortschronik wollte sich eine Ortsgemeinde als Herausgeberin versichern, dass mit bestimmten Inhalten nicht das Recht auf informationelle Selbstbestimmung Einzelner verletzt wird. Gegenstand eines Kapitels ist eine rund 160 Gebäude umfassende Häuser- und Familienchronik. Einem Auszug aus der Druckvorlage konnte der LfD entnehmen, dass die einzelnen Häuser mit Straßenname und Hausnummer bezeichnet sowie die früheren bzw. aktuellen Hauseigentümer und Bewohner namentlich genannt werden. Gleichzeitig werden deren Geburts- und Todestag sowie der Tag der Eheschließung angegeben. Die Daten wurden durch Recherchen ehrenamtlich tätiger Personen in Archiven bzw. durch die Befragung von Einwohnerinnen und Einwohnern ermittelt. Auf diese Tätigkeit wurde im Mitteilungsblatt der Verbandsgemeinde hingewiesen und um Mitteilung gebeten, sofern eine Bekanntgabe der Daten von Einwohnerinnen und Einwohnern nicht erwünscht ist. Auskünfte für die Ortschronik seitens der Verbandsgemeindeverwaltung erfolgten nicht.

Der Inhalt der Häuserchronik war vor der Veröffentlichung im Hinblick auf verschiedene Gesichtspunkte zu überprüfen. Wegen der zum Teil mehrere Jahrhunderte zurückreichenden Angaben war zunächst darauf hinzuweisen, dass das LDSG nur lebende Einzelpersonen als mögliche Inhaber des Rechts auf informationelle Selbstbestimmung schützt. Daten bereits Verstorbener werden nur vom nachwirkenden Grundrechtsschutz erfasst, der aufgrund des vorliegenden Sachverhalts jedoch nicht tangiert wurde. Wenn Informationen zu bereits verstorbenen Personen aus öffentlichen Archiven (§ 2 LArchG) gewonnen wurden, sind zusätzlich ggf. archivrechtliche Vorschriften zu beachten. Die Nutzung von Archivgut erfasst auch die Veröffentlichung von Daten. Archivgut darf, soweit es sich auf natürliche Personen bezieht, erst 30 Jahre nach deren Tod, oder, wenn das Todesjahr dem Archiv nicht bekannt ist, erst 110 Jahre nach der Geburt des Betroffenen benutzt werden (§ 3 Abs. 3 Satz 2 LArchG). Diese Sperrfrist kann ggf. verkürzt werden. Die Verarbeitung von durch Befragung gewonnenen personenbezogenen Daten lebender Personen bis hin zu deren Übermittlung im Rahmen der Veröffentlichung der Chronik bedarf einer Rechtsgrundlage. Dabei ist zu berücksichtigen, dass ohne Rechtsgrundlage erhobene Daten nicht weiter verwertet werden dürfen. Als Rechtsgrundlage für die Datenverarbeitung kam aufgrund des geschilderten Sachverhalts zunächst die Erteilung einer Einwilligung durch die Betroffenen in Betracht. Diese Einwilligung hätte darin gesehen werden können, dass die Betroffenen nach einer Information durch die ehrenamtlich Tätigen, wobei insbesondere auf die beabsichtigte Veröffentlichung im Rahmen einer

Chronik hinzuweisen gewesen wäre, mündlich Auskunft erteilt haben. Diese Einwilligung hätte auch von Eltern geäußerte Angaben zu ihren erwachsenen bzw. minderjährigen, aber bereits einsichtsfähigen Kindern erfasst, da insoweit aufgrund der familiären Verbindung von einer entsprechenden Vertretungsbefugnis ausgegangen werden konnte.

Anders zu beurteilen war allerdings die Erhebung personenbezogener Daten von aktuellen oder früheren Mietern bei den Hauseigentümern. Die Verarbeitung dieser Daten durch die Gemeinde und somit auch die Veröffentlichung wäre nur zulässig gewesen, wenn eine Einwilligung der Mieter selbst vorlag. Eine Einwilligung konnte auch nicht dadurch herbeigeführt werden, dass sich ein Mieter auf den oben erwähnten Hinweis im Mitteilungsblatt der Verbandsgemeinde nicht geäußert hat. Eine Grundlage für eine zulässige Datenübermittlung auf diesem Weg hätte allenfalls in § 16 Abs. 1 Nr. 4 LDSG hinsichtlich allgemein zugänglicher Daten gesehen werden können, die beispielsweise aus einem Telefonbuch gewonnen wurden. Das in der Vorschrift für die Datenübermittlung geforderte öffentliche Interesse hätte damit begründet werden können, dass die Herausgabe einer Chronik der Stärkung der gemeindlichen Identität und des Zusammengehörigkeitsgefühls dient. Allerdings wären davon nicht die personenbezogenen Daten derjenigen Personen erfasst worden, die nicht im Gebiet der Verbandsgemeinde leben und deshalb nur ausnahmsweise von einem entsprechenden Hinweis im Mitteilungsblatt hätten Kenntnis nehmen können.

9. Umweltschutz

Namensnennung im Planfeststellungsverfahren

Einem behördlichen Datenschutzbeauftragten fiel auf, dass in einem überörtlichen Planfeststellungsbeschluss neben den Stellungnahmen von Behörden auch die Namen und Adressen derjenigen genannt wurden, die Einwendungen gegen den Plan erhoben hatten. Er bat den LfD um Stellungnahme.

Die Regelungen im Verwaltungsverfahrensgesetz zum Planfeststellungsverfahren (§§ 72 ff.) sehen vor, dass die Anhörungsbehörde Einwendungen und Stellungnahmen der Behörden zu dem Plan mit dem Träger des Vorhabens, den Behörden, den Betroffenen und den Einwendern erörtert. Die Person, die Einwendungen erhoben hat, wird in diesem Erörterungstermin den Beteiligten bekannt. Der Planfeststellungsbeschluss mit den Entscheidungen über die Einwendungen ist sodann dem Träger des Vorhabens, den bekannten Betroffenen und den Einwendern zuzustellen. Der Beschluss ist zudem öffentlich auszulegen (§ 74 Abs. 4 VwVfG). Die Zustellung kann auch durch öffentliche Bekanntmachung erfolgen (§ 74 Abs. 5 VwVfG). Dies bedeutet, dass die Namen der Einwender, wenn sie im Planfeststellungsbeschluss genannt sind, ebenfalls veröffentlicht und damit den Kreis der Beteiligten verlassen würden. Eine solche Datenübermittlung wäre nur unter den Voraussetzungen von § 16 LDSG zulässig. Dann müsste die Veröffentlichung für die Aufgabenerfüllung der Planfeststellungsbehörde erforderlich sein. Diese Erforderlichkeit war nicht zu erkennen. Die Einwendungen und ihre Behandlung im Feststellungsverfahren können ohne Nennung von Namen und Adresse aufgeführt werden. Dabei kann sich u.U. aus anderen Informationen ein Bezug zur Person des Einwenders ergeben. Eine generelle ausdrückliche Nennung des Namens des Einwenders hielt der LfD aber grundsätzlich nicht für zulässig.

10. Gesundheitswesen

10.1 Elektronische Gesundheitskarte

Anders als in § 291a Abs. 1 SGB V vorgesehen ist die elektronische Gesundheitskarte nicht zum 1.1.2006 Realität für die gesetzlich Versicherten in der Bundesrepublik Deutschland geworden. Das ist auch gut so, denn die technische Umsetzung der in den rechtlichen Vorgaben enthaltenen Anforderungen ist alles andere als trivial und bedarf angesichts der damit verbundenen Auswirkungen gerade auf das informationelle Selbstbestimmungsrecht der Versicherten einer sorgfältigen und umsichtigen Vorgehensweise. Mit dem nun angestrebten Zeithorizont einer flächendeckenden Kartenausgabe mit eingeschränktem Anwendungsprofil frühestens im Laufe der Jahre 2008/2009 bleibt noch Zeit, die aus den Testläufen gewonnenen Erkenntnisse vor einem ersten Roll-Out der Karte angemessen zu berücksichtigen und zudem die aus der Sicht des Datenschutzes noch offenen Gesichtspunkte zu klären. Es bleibt abzuwarten, inwieweit diese Chance genutzt wird.

10.1.1 Entwicklung auf Bundesebene

Auf Bundesebene ist der BfDI permanent in die mit der Einführung der elektronischen Gesundheitskarte verbundenen Prozesse involviert. Hierzu gehören insbesondere die Einbindung in die in diesem Zusammenhang erforderliche Rechtsetzung sowie die inhaltliche Abstimmung mit dem BMG und der Gesellschaft für Telematik (gematik) zu Fragen der technischen Ausgestaltung der zu schaffenden Telematikinfrastruktur. Näheres hierzu kann dem Internetangebot des BfDI unter der Adresse http://www.bfdi.bund.de/nn_531516/DE/Schwerpunkte/ElektronischeGesundheitskarte/eGK__node.html__nnn=true entnommen werden.

Datenschutz hat nach Aussage aller mit der Gestaltung der elektronischen Gesundheitskarte befassten Akteure einen hohen Stellenwert. Man ist sich einig, dass die mit der Einführung der elektronischen Gesundheitskarte erwarteten medizinischen und ökonomischen Vorteile in hohem Maße von der Nutzung der freiwilligen Anwendungen der Karte – wie z.B. der elektronischen Patientenakte – abhängen. Der LfD teilt die Auffassung, dass die hierzu notwendige Akzeptanz bei den Versicherten nur dann zu erreichen ist, wenn die Sicherheit und Vertrauenswürdigkeit der bereit gestellten Telematikinfrastruktur sowie eine umfassende und unkomplizierte Wahrnehmung der Betroffenenrechte gewährleistet sind. Aus der heutigen Sicht sind deshalb im Rahmen des Einführungsprozesses insbesondere folgende Aspekte noch klärungsbedürftig:

- Ein konkreter Zeitplan für die Testung der aus datenschutzrechtlicher Sicht besonders bedeutsamen Anwendung einer elektronischen Patientenakte in den Modellregionen ist bislang noch nicht festgelegt worden. Es steht damit noch nicht fest, wann die Funktionsfähigkeit der Anwendung und der in diesem Zusammenhang erforderlichen Sicherheitselemente erprobt werden.
- Es ist noch offen, welche Stellen für den Einsatz der elektronischen Gesundheitskarte nach § 291a SGB V und der damit zusammenhängenden Verarbeitung von Daten datenschutzrechtlich verantwortlich sind. Dies ist deshalb von Bedeutung, da die Kontrollzuständigkeit der Datenschutzaufsicht an die Identität der verantwortlichen Stelle anknüpft. In Betracht kommen beispielsweise die Krankenkassen, die die Gesundheitskarten an die Versicherten herausgeben, und die gematik, die die erforderliche Telematikinfrastruktur betreibt.
- Die Rahmenbedingungen für einen Zugriff der Versicherten auf die über sie gespeicherten Daten müssen geklärt werden. So wird zwischen den Datenschutzbeauftragten des Bundes und der Länder derzeit kontrovers diskutiert, ob den Versicherten auch von zu Hause aus ein Zugriff auf diese Daten eingeräumt werden darf. Der LfD tritt in diesem Zusammenhang auch für die Ermöglichung eines häuslichen Zugangs der Versicherten auf die sie betreffenden Daten ein, sofern technische Lösungen die gesetzlichen Vorgaben für einen Zugriff einhalten. Aber auch Fragen zur Handhabung anderer Betroffenenrechte wie das Verbergen und Löschen von Einträgen beispielsweise im Zusammenhang mit dem elektronischen Rezept sind noch nicht abschließend beantwortet.

10.1.2 Entwicklung in Rheinland-Pfalz

Im Berichtszeitraum begleitete der LfD die verschiedenen in Rheinland-Pfalz im Zusammenhang mit der elektronischen Gesundheitskarte stehenden Vorhaben.

- Modellprojekt „Elektronische Gesundheitskarte Rheinland-Pfalz“
  Das Projekt testet in der Region Trier auf der Grundlage der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte den Einsatz der von der gematik spezifizierten Komponenten in den zunächst dafür vorgesehenen Anwendungen. Am 3.9.2007 begann mit dem Start des 10.000er-Feldtests in der Modellregion eine weitere Phase auf dem Weg zur Einführung der elektronischen Gesundheitskarte. Derartige Tests finden zeitversetzt in bundesweit sieben Modellregionen (neben Trier auch in Flensburg, Ingolstadt, Heilbronn, Bochum/Essen, Wolfsburg und Löbau/Zittau) statt. Basierend auf der o.g. Testverordnung sollen diese Feldtests die Einsetzbarkeit des Gesamtsystems unter realen Einsatzbedingungen nachweisen und den Einfluss auf bestehende Geschäftsprozesse erfassen. Der LfD wird die zu erwartenden Testergebnisse bewerten und gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder in den weiteren Ausgestaltungsprozess der elektronischen Gesundheitskarte einbringen.

- Modellversuch „Sektorenübergreifende Patientenakte“
  Das bereits seit mehreren Jahren in der Region Trier bestehende Projekt, das in der Vergangenheit als Modellprojekt „Elektronische Gesundheitskarte Rheinland-Pfalz“ bezeichnet wurde (vgl. 20. Tb., Tz. 10.1.2), testet die aus datenschutzrechtlicher Sicht wichtige Anwendung einer elektronischen Patientenakte. Angesichts des bislang noch nicht festgelegten Zeitplans für die Spezifizierung und bundesweite Testung der Anwendung kommt dem in Trier angesiedelten Vorhaben eine besondere Bedeutung zu.

– Projekt „ePA junior“
  Ergänzend zu den genannten Projekten soll ab 1.1.2008 flächendeckend in Rheinland-Pfalz eine elektronische Patientenakte für Kinder („ePA junior“) angeboten werden. Nach den bislang dem LfD bekannten Vorstellungen soll das im Juli 2007 angekündigte Vorhaben, das sich an alle im Jahre 2008 in Rheinland-Pfalz Neugeborenen richtet, auf der gleichen Technik basieren, die bereits dem o.g. Modellversuch einer sektorenübergeifenden Patientenakte zugrunde liegt. Die für eine datenschutzrechtliche Bewertung des Vorhabens erforderlichen weiteren Einzelheiten werden dem LfD von den Projektinitiatoren (MASGFF und Firma Compugroup) allerdings noch dargelegt werden.

10.2 Ärztliche Schweigepflicht gegenüber Drittbetroffenen

Einer Bitte der Landesärztekammer folgend nahm der LfD in einem Beitrag für das rheinland-pfälzische Ärzteblatt zur Problematik sinngemäß wie folgt Stellung:

Die ärztliche Schweigepflicht wird regelmäßig mit dem Hippokratischen Eid und weniger mit dem Begriff des Datenschutzes in Verbindung gebracht. Dabei stellt dieses mehr als 2000 Jahre alte Gelöbnis des Arztes, über all das Stillschweigen zu bewahren, was er bei der Behandlung Kranker erfährt, eine der ältesten Datenschutzregeln überhaupt dar. Der besondere Schutz des Arzt-Patienten-Verhältnisses hat auch im heutigen Recht einen besonderen Stellenwert: Der Gesetzgeber hat dieses Berufsgeheimnis gleich dreifach, nämlich mit der Strafbewehrung einer unbefugten Offenbarung von Patientendaten (§ 203 Abs. 1 StGB), dem Zeugnisverweigerungsrecht (§ 53 StPO) und dem Beschlagnahmeverbot (§ 97 StPO) geschützt. Auch in § 9 der Berufsordnung der Ärzte, die als Satzung von der Landesärztekammer erlassen wird, sind Schweigepflichten festgeschrieben. Diese standesrechtliche Regelung ist kein bloßer Ehrenkodex, sondern für Ärzte genauso bindend wie Verfassung, Gesetze und Rechtsverordnungen.

Die ärztliche Schweigepflicht ist unter zwei Gesichtspunkten von Bedeutung: Zum einen bildet sie die Grundlage für eine erfolgreiche Behandlung, weil sich der Patient im Vertrauen auf die Verschwiegenheit des Arztes rückhaltlos offenbaren kann. Zum anderen liegt sie im öffentlichen Interesse, da durch eine effektive Behandlung die wirtschaftlichen und sozialen Folgen von Krankheiten begrenzt werden können. Zum Schutzgegenstand der Schweigepflicht gehören nicht nur die bei der Behandlung des Patienten anfallenden Anamnese-, Befund- und Diagnoseangaben. Auch Informationen über Rahmenbedingungen des Arzt-Patientenverhältnisses, wie z.B. die bloße Tatsache, dass sich jemand überhaupt in ärztlicher oder psychologischer Behandlung befindet oder stationär aufgenommen wurde, begründen ein Geheimhaltungsinteresse des Patienten. Die Pflicht zur Wahrung der Schweigepflicht gilt jedoch nicht uneingeschränkt: Eine Offenbarung von Patientendaten beispielsweise bei der Abrechnung medizinischer Leistungen oder bei der Verordnung von Heil- und Hilfsmitteln ist für das Funktionieren des Gesundheitssystems unerlässlich. Die Weitergabe von Patientendaten ist aber stets nur im erforderlichen Umfang und auch nur dann zulässig, wenn entweder die Einwilligung des Patienten vorliegt oder eine normenklare Rechtsgrundlage die Datenweitergabe stützt. Auch bei Vorliegen sonstiger allgemeiner Rechtfertigungsgründe darf der Arzt Patientendaten offenbaren, z.B. Wahrnehmung eigener berechtigter Interessen im Rahmen einer Honorarklage; Unterrichtung des Lebenspartners eines HIV-Patienten (OLG Frankfurt NJW 2000, S. 875); Offenbarung von Patientendaten bei begründetem Verdacht einer Misshandlung, eines Missbrauchs oder einer schwerwiegenden Vernachlässigung (§ 9 Abs. 2 der Berufsordnung). Der Patient soll sich also darauf verlassen können, dass seine Daten durch den Arzt nur bei Vorliegen dieser Übermittlungsvoraussetzungen Außenstehenden gegenüber offenbart werden.

Zu einer Kollision mit den Datenschutzrechten eines Dritten kann es aber dann kommen, wenn der Patient im Rahmen seiner Behandlung personenbezogene Daten über einen Dritten (z.B. im Rahmen der Familienanamnese) mitgeteilt hat und diese Daten in die Patientenakte aufgenommen werden. Die Geltendmachung von Datenschutzrechten (insbesondere Auskunft, Berichtigung, Sperrung und Löschung personenbezogener Daten) ist dem „Betroffenen“ im Sinne des Datenschutzrechts vorbehalten. Dies ist die Person, über deren persönliche oder sachliche Verhältnisse eine Aussage getroffen wird (§ 3 Abs. 1 BDSG, § 3 Abs. 1 LDSG). Unstreitig ist der Patient „Betroffener“ in Bezug auf seine eigenen Daten. Stehen Patientendaten jedoch in Beziehung zu anderen Personen, stellt sich die Frage, ob sich diese als „Betroffene“ ebenfalls auf Datenschutzrechte berufen können.

Nur vereinzelt hat der Gesetzgeber Regelungen zum Datenschutz bei Drittbezogenheit getroffen: § 15 Abs. 5 BDSG (§ 13 Abs. 5 LDSG, § 67d Abs. 3 SGB X) knüpft beispielsweise rechtliche Folgerungen daran an, dass Angaben über einen Betroffenen mit weiteren personenbezogenen Daten eines Dritten so verbunden sind, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist. In diesen Fällen ist die Verarbeitung der Daten Dritter nur zulässig, wenn deren schutzwürdige Interessen an der Geheimhaltung nicht überwiegen. Damit ist aber noch keine Aussage darüber getroffen, ob eine Beziehungsperson als Betroffener Auskunft über die eigenen Daten verlangen kann und wie mit ihren Daten im Übrigen zu verfahren ist.

In einem Fall, mit dem sich sämtliche in Betracht kommenden Aufsichtsbehörden befassen mussten, enthielt ein Arztbrief die Feststellung, die Geschwister des Patienten seien psychisch krank, wobei nicht darauf hingewiesen wurde, dass diese Information auf der subjektiven Einschätzung des Patienten beruhte. Als die Geschwister davon erfuhren, machten sie Auskunfts-, Berichtigungs- und Löschungsansprüche geltend. Die Aufsichtsbehörden hatten sich mit der Frage zu befassen, welche Informationen im Arztbrief übermittelt werden durften und ob der Arztbrief – so wie gefordert – in Bezug auf die Geschwister korrigiert bzw. unkenntlich zu machen war.

Stehen Daten in Beziehung zu mehreren Personen, ist zu differenzieren: Handelt es sich um Angaben, Einschätzungen oder Wertungen über einen Dritten, ohne dass eine nähere Beziehung zu der Primärperson vorliegt (z.B. Äußerungen über allgemein bekannte Personen des öffentlichen Lebens) oder um solche Daten, die in erster Linie das Verhältnis der Primärperson zu einem Dritten betreffen (z.B. Steuerklasse bei Eheleuten), ist der Dritte nicht „Betroffener“ im Sinne des Datenschutzrechts. Diese Personen können daher keine Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsansprüche geltend machen. Stehen hingegen der originär Betroffene und ein Dritter in einem konkreten Verhältnis zueinander, dann haben Informationen über die Art der Beziehung und die Bezeichnung der Beziehungsperson einen doppelten Bezug, so dass sowohl der originär Betroffene als auch die Beziehungsperson „Betroffene“ im Sinne des Datenschutzrechts sind (s. Dammann in: Simitis, Kommentar zum BDSG, § 3 Rdnr. 43). MDK-Akten enthalten beispielsweise Angaben sowohl über den Versicherten als auch über den behandelnden Arzt. Aufgrund dieses Doppelbezugs sind beide Beteiligte als „Betroffene“ anzusehen. In dem o.g. Fall waren die Geschwister „Betroffene“ und konnten daher Datenschutzrechte geltend machen.

Drittbetroffene haben zwar nicht das Recht, Einsicht in die Patientenakte eines anderen zu nehmen, sie können aber nach allgemeinem Datenschutzrecht Auskunft über die zu ihrer Person gespeicherten Daten verlangen (§ 34 BDSG, § 18 LDSG). Dies beinhaltet auch das Recht, darüber unterrichtet zu werden, an welche Personen oder Stellen sie betreffende Informationen übermittelt wurden. Handelt es sich – so wie hier – um objektiv unrichtige Daten, besteht darüber hinaus ein Berichtigungs- bzw. Löschungsanspruch (§ 35 BDSG, § 19 LDSG) nicht nur gegenüber dem Behandler, sondern auch gegenüber den Personen oder Stellen, an die diese Daten übermittelt worden sind. Da der Arztbrief im vorliegenden Fall an das Gesundheitsamt geschickt worden war, musste auch hier eine Löschung der fraglichen Textpassage vorgenommen werden.

Für die Praxis bedeutet dies, dass dem Erforderlichkeitsgrundsatz bei Datenübermittlungen eine besondere Bedeutung zukommt. Nur die Informationen, die der Empfänger für seine Aufgaben tatsächlich benötigt, dürfen weitergegeben werden. Bei Daten aus der Familienanamnese oder subjektiven Einschätzungen des Patienten ist dabei ein besonders strenger Maßstab anzulegen. Wenn es gleichwohl erforderlich sein sollte, Daten über Dritte mitzuteilen, sollten keine personenbezogenen Informationen, sondern anonymisierte Angaben (z.B. „familiäre Vorbelastung“, „ein Freund der Patientin“...) gewählt werden. In Zweifelsfällen besteht für niedergelassene Ärzte die Möglichkeit, die ADD als zuständige Datenschutzaufsichtsbehörde mit solchen Fragen zu befassen. Ärzte, die bei öffentlichen Stellen des Landes beschäftigt sind, können sich an den behördlichen Datenschutzbeauftragten oder an den LfD wenden.

10.3 Aufgaben der Berufskammern im Zusammenhang mit der Aufbewahrung ärztlicher Unterlagen nach Insolvenz einer Arztpraxis

Im Berichtszeitraum war der LfD mit der Frage befasst, welche Aufgaben den Berufskammern im Zusammenhang mit der Aufbewahrung ärztlicher Unterlagen nach Insolvenz einer Arztpraxis zukommen.

Im zugrunde liegenden Sachverhalt hatte die insolvent gewordene Ärztin ihre gemieteten Praxisräume kurzfristig verlassen, ohne darin befindliche Patientenunterlagen entsprechend den berufsrechtlichen Vorgaben zu sichern bzw. für deren weitere Aufbewahrung zu sorgen. Die Unterlagen, u.a. Röntgenbilder und Untersuchungsbefunde, befanden sich daher weiterhin in den dem Vermieter bzw. dessen Hausmeister zugänglichen Räumlichkeiten. Nach Einschätzung der Bezirksärztekammer, die den LfD über den Fall unterrichtet hatte, konnte die betroffene Ärztin mangels tatsächlicher und finanzieller Möglichkeiten ihren Berufspflichten nicht nachkommen; spätestens bei Weitervermietung der Räume sei ein Zugriff durch unbefugte Dritte auf die Unterlagen zu befürchten gewesen. Der LfD vertrat gegenüber der betroffenen Ärztekammer die Auffassung, dass diese nach § 3 Abs. 1 Satz 3 Nr. 3 HeilBG verpflichtet ist, die zur Beseitigung eines berufsrechtswidrigen Zustands notwendigen Maßnahmen selbst zu treffen, sofern das Kammermitglied der Erfüllung seiner Berufspflichten nicht nachkommt. Angesichts der konkreten Umstände war im Hinblick auf einen umfassenden Schutz der Patientendaten ein sofortiges Tätigwerden der Kammer geboten. Insbesondere war dafür Sorge zu tragen, dass die betroffenen Unterlagen unverzüglich der tatsächlichen Zugriffsmöglichkeit unbefugter Dritter entzogen und entsprechend den berufsrechtlichen Vorgaben aufbewahrt werden. Diese Auffassung teilte die betroffene Bezirksärztekammer nicht. Vielmehr war sie der Ansicht, dass die gesetzliche Regelung keine Verpflichtung der Kammern beinhaltet, in Einzelfällen, in denen die Kammermitglieder die ihnen obliegenden Berufspflichten trotz Aufforderung nicht einhalten, selbst ggf. Maßnahmen zur Herstellung berufsrechtsgemäßer Zustände z.B. im Rahmen der Ersatzvornahme treffen zu müssen. Aus diesem Grunde lehnte sie auch ein entsprechendes Tätigwerden in dem zugrunde liegenden Fall ab.

Zur weiteren Klärung der Angelegenheit hat sich der LfD an das zuständige Gesundheitsministerium gewandt. Dieses teilt grundsätzlich die vom LfD vertretene Rechtsauffassung und beabsichtigt, die Problematik zu einem Thema der nächsten Sitzung der Bund-Länder-Arbeitsgruppe „Berufe des Gesundheitswesens“ zu machen. Eine vorläufige Erörterung mit der Bundesärztekammer habe jedoch ergeben, dass diese in Abstimmung mit den Landesärztekammern einer derartigen Handlungspflicht der Kammern eher ablehnend gegenüber stehe. Die Landesärztekammern sähen sich grundsätzlich nicht in der Lage, die in Rede stehende Aufgabe zu übernehmen. Nur vereinzelt bestehe die Bereitschaft, gegen vollständige Kostenerstattung entsprechend tätig zu werden. In dem zugrunde liegenden Einzelfall hatte sich zwischenzeitlich die Landesärztekammer zur Aufbewahrung der ärztlichen Unterlagen bereit erklärt, so dass ein weiterer Handlungsbedarf nicht mehr bestand. Der LfD wird sich dennoch um eine grundsätzliche Klärung der Fragestellung bemühen. Angesichts der hohen Schutzbedürftigkeit der betroffenen Daten und einer zunehmenden Zahl solcher Fälle muss feststehen, wer für die datenschutzgerechte Aufbewahrung der ärztlichen Unterlagen verantwortlich ist.

10.4 Externe Verarbeitung von Patientendaten im Krankenhausbereich

Die Auslagerung der Verarbeitung von Patientendaten und insbesondere die externe Archivierung von Altakten aus dem Krankenhausbereich steht bereits seit geraumer Zeit im Fokus der datenschutzrechtlichen Diskussion. Ausgehend von der in § 36 Abs. 9 LKG enthaltenen Regelung hatte sich der LfD bereits in seinem 16. Tb. (Tz. 10.4.1) und 20. TB (Tz. 10.6.2) ausführlich zu der Thematik geäußert. Im Ergebnis war hiernach eine Auftragsdatenverarbeitung auf der Basis der o.g. Regelung bei bestehender Zugangsmöglichkeit des Auftragnehmers zu den Patientendaten nur zulässig, wenn es sich bei diesem um eine ärztlich geleitete Einrichtung oder eine sonstige der Strafandrohung des § 203 Abs. 1 und 3 StGB unterliegende Stelle handelt. Dagegen war nach Auffassung des LfD eine in diesem Zusammenhang angestrebte externe Verarbeitung von Patientendaten durch einen anderen Auftragnehmer, dessen Mitarbeiter lediglich nach dem Verpflichtungsgesetz förmlich verpflichtet wurden, datenschutzrechtlich nicht hinnehmbar. Denn anders als bei den Stellen, die der Strafandrohung des § 203 Abs. 1 und 3 StGB unterliegen, sind im Falle der förmlichen Verpflichtung des Auftragnehmers die im Auftrag verarbeiteten Daten weder durch ein strafprozessuales Zeugnisverweigerungsrecht noch durch ein Beschlagnahmeverbot geschützt waren. Von einer § 203 StGB entsprechenden Schweigepflicht, wie sie in § 36 Abs. 9 LKG verlangt wird, konnte daher nicht ausgegangen werden.

In der Zwischenzeit hat sich die Rechtslage jedoch trotz unveränderter Fassung des § 36 Abs. 9 LKG maßgeblich geändert. Mit Inkrafttreten des Gesundheitsmodernisierungsgesetzes wurde u.a. auch die Regelung des § 97 Abs. 2 StPO zum strafprozessualen Beschlagnahmeverbot ausgeweitet. Anders als bisher unterliegen nach § 97 Abs. 2 Satz 2 StPO u.a. nun auch solche Gegenstände der Beschlagnahme nicht, auf die sich das Zeugnisverweigerungsrecht der Ärzte erstreckt, wenn sie im Gewahrsam eines Dienstleisters sind, der für einen Arzt personenbezogene Daten verarbeitet. Im Hinblick auf eine beabsichtigte Auftragsdatenverarbeitung im Krankenhausbereich hat dies zur Folge, dass nunmehr die bei dem nach dem Verpflichtungsgesetz förmlich verpflichteten Auftragnehmer verarbeiteten Patientendaten einen der ärztlichen Schweigepflicht vergleichbaren Schutz genießen.

Im Ergebnis hält daher der LfD angesichts der dargestellten Rechtsentwicklung seine bisherigen datenschutzrechtlichen Bedenken im Zusammenhang mit einer auf der Grundlage des § 36 Abs. 9 LKG erwogenen externen Verarbeitung von Patientendaten nicht mehr aufrecht, sofern es sich bei dem in Frage kommenden Auftragnehmer um eine der Strafandrohung des § 203 Abs. 2 Satz 1 Nr. 2 StGB unterliegende Stelle handelt.

10.5 Datenschutz im Schlichtungsverfahren

Aufgrund einer Eingabe hatte sich der LfD im Berichtszeitraum erneut mit der Frage zu befassen, ob sich der Arzt, dem ein Behandlungsfehler vorgeworfen wird, mit dem Nachbehandler in Verbindung setzen darf, um sich über den weiteren Behandlungsverlauf zu erkundigen. Eine Petentin trug vor, dieser Informationsvorgang, der ohne ihre Kenntnis und Billigung erfolgte, habe den Ausgang des Schlichtungs- und Gerichtsverfahrens zu ihrem Nachteil vorentschieden. Bekanntlich hacke eine Krähe der anderen kein Auge aus.

Aus Zuständigkeitsgründen konnte der LfD im vorliegenden Fall nur zur Zulässigkeit der Datenerhebung seitens der Klinik Stellung nehmen, denn das übermittelnde Krankenhaus hatte seinen Sitz in Hessen. Als Rechtsgrundlage für die Erhebung personenbezogener Patientendaten seitens der Klinik kam im vorliegenden Fall allein § 36 Abs. 2 Ziff. 1 LKG in Betracht, wonach die Erhebung von Patientendaten u.a. dann zulässig ist, soweit dies im Rahmen des Behandlungsverhältnisses auf vertraglicher Grundlage erforderlich ist. Entgegen seiner früher vertretenen Rechtsauffassung geht der LfD nunmehr davon aus, dass spätestens mit einer von Patientenseite beantragten Einleitung eines Schlichtungsverfahrens der Behandlungsvertrag mit dem Krankenhaus bzw. dem Klinikum als beendet angesehen werden muss und folglich Informationsvorgänge hierauf nicht mehr gestützt werden können. Der LfD verkennt dabei nicht, dass der eines Behandlungsfehlers bezichtigte (Zahn)Arzt die Möglichkeit haben muss, sich gegen die erhobenen Vorwürfe zu verteidigen und ihm insofern auch aktuelle Behandlungsunterlagen seines ehemaligen Patienten zur Verfügung zu stellen sind. Dies soll jedoch ausschließlich über den Schlichtungsausschuss, und

zwar auf der Basis einer mit dem LfD abgestimmten Einwilligungserklärung des Betroffenen erfolgen. Hierin erklärt sich der Patient mit der Weitergabe von medizinischen Daten durch den Schlichtungsausschuss an die anderen Beteiligten des Schlichtungsverfahrens ausdrücklich einverstanden.

Im Hinblick darauf, dass das Schlichtungsverfahren von der Zustimmung des (Zahn)Arztes abhängt, sieht der LfD keine unangemessene Benachteiligung darin, wenn diesem die eigenständige Kontaktaufnahme mit dem Nachbehandler verwehrt ist. In den dem LfD vorliegenden Petitionen wurde gerade dieser unmittelbare Informationsaustausch für den negativen Ausgang des Schlichtungs- bzw. Gerichtsverfahrens verantwortlich gemacht. Unter dem Gesichtspunkt der Transparenz, aber auch um bereits dem Anschein eines kollusiven Zusammenwirkens zum Nachteil des Patienten entgegenzutreten, hält der LfD die geschilderte Verfahrensweise für geboten. Hinzu kommt, dass ein nachbehandelnder (Zahn)Arzt schon aufgrund der berufsrechtlichen Regelungen nicht vom Einverständnis des Patienten in die Datenübermitttlung ausgehen kann. Ein entsprechendes Auskunftsbegehren der Klinik würde somit einem rechtswidrigen Verhalten Vorschub leisten.

Die Datenerhebung kann daher nicht auf den Behandlungsvertrag gestützt werden. § 36 Abs. 2 Ziff. 1 LKG scheidet somit als Rechtsgrundlage aus. Da eine andere Rechtsvorschrift nicht in Betracht kommt und auch nicht von der Einwilligung des Betroffenen ausgegangen werden kann, war die Datenerhebung im Ergebnis unzulässig. Der hessische Datenschutzbeauftragte, der sich mit der Zulässigkeit der Datenübermittlung seitens der hessischen Klinik zu befassen hatte, kam zu demselben Ergebnis, so dass der Informationsvorgang insgesamt als rechtswidrig zu bewerten war. Die rheinland-pfälzische Klinik schloss sich der Rechtsauffassung des LfD an, so dass zumindest in künftigen Fällen eine Verbesserung des Datenschutzes in Schlichtungsfällen erreicht werden konnte. Für die Petentin kam diese Einsicht freilich zu spät: Vor Gericht hatte sie mit ihrer Klage keinen Erfolg. Die Frage der Verwertbarkeit unzulässig übermittelter Informationen wurde dabei vom Richter nicht ansatzweise geprüft.

11. Sozialdatenschutz

11.1 Grundsicherung für Arbeitsuchende – Datenschutz bei Hartz IV

Erwartungsgemäß hat sich im Berichtszeitraum die unter dem Namen Hartz IV bekannt gewordene Grundsicherung für Arbeitsuchende nach dem SGB II als Dauerbrenner in Sachen Datenschutz herausgestellt. Soweit sich der BfDI auf Bundesebene im Rahmen der Gesetzgebung sowie bei der Gesetzesauslegung und der dafür erforderlichen Abstimmung mit der BA um die Gewährleistung des Datenschutzes gekümmert hat, kann Näheres dem Internetangebot des BfDI und insbesondere den Tätigkeitsberichten unter der Adresse http://www.bfdi.bund.de/cln_029/nn_531940/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TaetigkeitsberichteDesBFD.html entnommen werden.

Den LfD beschäftigten neben zahlreichen Eingaben auch grundsätzliche Fragestellungen wie z.B. die Klärung der Zuständigkeiten zwischen dem BfDI und den Landesbeauftragten im Zusammenhang mit der Ausübung der Datenschutzkontrolle bei den ARGEn oder die Erfüllung allgemeiner datenschutzrechtlicher Pflichten durch diese. Im Rahmen der örtlichen Feststellungen wurden die beiden in Rheinland-Pfalz zugelassenen kommunalen Träger (sog. Optionskommunen) sowie einige ARGEn besucht. Dabei konnte der LfD im Hinblick auf die Einhaltung der datenschutzrechtlichen Vorgaben keine wesentlichen Unterschiede zwischen den beiden Verfahrensmodellen feststellen.

11.1.1 Ausübung der Datenschutzkontrolle bei den ARGEn

Die Frage der datenschutzrechtlichen Kontrollzuständigkeit bei den ARGEn ist so alt wie das SGB II. Zunächst verlief die Trennlinie der unterschiedlichen Sichtweisen zwischen den Datenschutzbeauftragten und der BA: während die Datenschützer einhellig der Auffassung waren, dass es sich bei dem neu geschaffenen Konstrukt einer Arbeitsgemeinschaft i.S.v. § 44b SGB II regelmäßig um eine öffentliche Stelle eines Landes handelt und deshalb der Kontrollkompetenz des jeweiligen Landesdatenschutzbeauftragten unterliegt, bestritt die BA eine derartige Sichtweise. Nach ihrer Ansicht stellten die ARGEn gerade keine eigenverantwortlich Daten verarbeitende Stellen dar, sondern lediglich eine besondere Organisationsform in der BA. Zuständig wäre demnach der BfDI gewesen. Zu einer Zuspitzung der Zuständigkeitsfrage kam es im Frühjahr 2006, nachdem eine Weisung der BA an die ARGEn dazu führte, dass örtliche Feststellungen nur noch eingeschränkt durchgeführt werden konnten. So verweigerte eine ARGE dem LfD im Rahmen einer Kontrolle den Zugriff auf die von ihr elektronisch verarbeiteten Daten. Die Prüfung musste abgebrochen werden.

Mit dem Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende, das zum 1.8.2006 in Kraft trat, missglückte dem Gesetzgeber leider die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt geforderte

Klarstellung der Zuständigkeitsfrage (vgl. Anlagen 3 und 10). Die in § 50 Abs. 2 SGB II aufgenommene Formulierung, wonach die BA verantwortliche Stelle nach § 67 Abs. 9 SGB X ist, soweit die ARGEn Aufgaben der Arbeitsagenturen wahrnehmen, führte bei einigen Landesbeauftragten zu dem Schluss, dass das Gesetz nun eindeutig die von den ARGEn insoweit durchgeführten Datenverarbeitungen in die Verantwortlichkeit der BA legte und folglich eine Datenschutzkontrolle nur durch den hierfür zuständigen BfDI erfolgen dürfe, sofern Aufgaben der BA wahrgenommen werden. Diese Auffassung teilt der LfD nicht. Denn maßgebliche Regelung für die Bestimmung der zuständigen Datenschutzaufsicht ist im Gefüge des Sozialgesetzbuchs § 83 SGB X. Nach Absatz 3 Satz 1 sind u.a. Arbeitsgemeinschaften, die auf der Grundlage des Sozialgesetzbuchs Aufgaben wahrnehmen, öffentliche Stellen der Länder, wenn sie nicht über den Bereich eines Landes hinaus tätig werden. Mit der in § 50 Abs. 2 SGB II enthaltenen Ergänzung hat der Gesetzgeber eine hiervon abweichende Datenschutzaufsicht weder konstituiert noch konstituieren wollen. Gerade die in § 44 b Abs. 1 Satz 1 SGB II normierte einheitliche Aufgabenwahrnehmung spricht gegen eine Aufspaltung der Datenschutzaufsicht.

Dem BfDI gelang es, in direkten Gesprächen mit der BA und dem BMAS die weiterhin offene Zuständigkeitsfrage einvernehmlich zu lösen. Danach ist der BfDI für die von der BA zentral entwickelten und von den ARGEn eingesetzten Verfahren zuständig, während die Landesdatenschutzbeauftragten die Datenverarbeitungen der einzelnen ARGEn kontrollieren. Dies stellt aus der Sicht des LfD eine sachgerechte Lösung dar und wird insbesondere den Interessen der betroffenen Hilfesuchenden nach einer effektiven Datenschutzkontrolle gerecht.

11.1.2 Erfüllung allgemeiner datenschutzrechtlicher Pflichten durch die ARGEn

Da zwischen den Datenschutzbeauftragten und der BA ein Dissens im Hinblick auf die Einordnung der ARGEn als eigenverantwortlich Daten verarbeitende Stellen besteht, werden von diesen auch die jede öffentliche Stelle i.S.v. § 2 Abs. 1 LDSG treffenden allgemeinen datenschutzrechtlichen Pflichten nicht oder nur sehr begrenzt erfüllt. Hierzu gehören insbesondere die Bestellung eines eigenen behördlichen Datenschutzbeauftragten und der Erlass einer Dienstanweisung zum technisch-organisatorischen Datenschutz. Die vom LfD nach jeder örtlichen Feststellung bei einer rheinland-pfälzischen ARGE angemahnte Einhaltung dieser Pflichten wurde bislang stereotyp durch die BA unter Hinweis auf die nach Auffassung der BA fehlende Eigenverantwortlichkeit der ARGEn abgelehnt.

Angesichts der in den ARGEn tagtäglich zu verarbeitenden Menge sehr schutzbedürftiger Daten ist dieser Zustand äußerst unbefriedigend. Die gegenwärtige Praxis verstößt gegen die Vorgaben des Landesdatenschutzgesetzes. Gerade die Bestellung eines eigenen behördlichen Datenschutzbeauftragten würde nach Einschätzung des LfD zur Stärkung des Datenschutzbewusstseins in den ARGEn beitragen und darüber hinaus zu einer effektiveren internen Verteilung datenschutzrelevanter Informationen führen.

11.1.3 Datenschutz bei der Gewährung des ALG II

Im Zusammenhang mit der Gewährung von Arbeitslosengeld II hat sich der LfD im Berichtszeitraum mit zahlreichen datenschutzrelevanten Problemstellungen befasst. Dazu gehörten u.a. folgende Fragen:

- Einsatz eigener Vordrucke
  Trotz der Existenz der von der BA entwickelten und mit den Datenschutzbeauftragten abgestimmten umfangreichen Antragsvordrucke muss ein hartnäckiges Bedürfnis der ARGEn nach weiteren Formularen konstatiert werden. So wurde der LfD immer wieder durch Eingaben auf diverse von den Verwaltungen selbst entworfene Vordrucke hingewiesen, die den datenschutzrechtlichen Anforderungen nicht hinreichend Rechnung getragen haben. Gravierendstes Beispiel war ein sog. Zusatzblatt zur Regelung des Wohnungsbetretungsrechts bei Außendienstprüfungen. Hiernach sollten alle Antragsteller bereits bei Antragstellung eine Erklärung darüber abgeben, ob sie damit einverstanden wären, dass die Mitarbeiter der ARGE im Rahmen gesetzlich vorgeschriebener Außendienstaufgaben ihre Wohnung bzw. ihr Haus außerhalb der Nachtzeiten betreten dürfen. Nach dem Vordruck hatte die Verneinung des Einverständnisses lediglich eine schriftliche Benachrichtigung der Antragsteller über einen festgelegten Besuchstermin zur Folge. Wie sich herausstellte, diente der Vordruck einem Kooperationstest der Betroffenen: Wer sich einverstanden erklärte, wurde als kooperativer und damit zuverlässiger Antragsteller eingeordnet. Eine derartige Vorgehensweise kollidiert bereits mit den Grundsätzen der Transparenz und Offenheit des Verwaltungshandelns. Zudem widerspricht es dem Erforderlichkeitsgrundsatz, routinemäßig von jedem Antragsteller bei Antragstellung dessen Einverständnis mit einem Hausbesuch der Mitarbeiter der ARGE abzufragen, obwohl zu diesem Zeitpunkt weder die sachliche Notwendigkeit einer derartigen Maßnahme noch der Inhalt der auf diese Weise zu erhebenden Daten ersichtlich sind. Da dem Antragsteller auch nicht dargelegt wird, ob und aus welchen Gründen im konkreten Fall ein Hausbesuch bei dem Betroffenen ein taugliches und angemessenes Mittel zur Sachverhaltsaufklärung ist, hat dieser keine Möglichkeit, die für seine Entscheidung über die Gewährung eines Wohnungszutritts maßgeblichen Gesichtspunkte zu erkennen und zu gewichten.

Auch der Einsatz sog. Mietbescheinigungen war immer wieder Gegenstand von an den LfD gerichteten Eingaben. In diesen regelmäßig von dem Vermieter zu unterzeichnenden Vordrucken wurden detaillierte Angaben zur Miete und den darin enthaltenen Kostenbestandteilen sowie allgemeine Informationen zur Wohnung, der Ausstattung, der Beheizungsart und einer eventuellen öffentlichen Förderung erfragt. Zugleich sollte der Vermieter neben seinem Namen auch seine Anschrift und Telefonnummer angeben. Datenschutzrechtlich bestehen hiergegen Bedenken. So werden im Rahmen des von den ARGEn eingesetzten Zusatzblatts 1 zu Abschnitt V des von der BA erstellten Hauptantrags bereits etliche in der o.g. Mietbescheinigung erbetene Informationen abgefragt (Angaben über die Wohnung einschließlich der erstmaligen Bezugsfertigkeit, die Höhe der Kaltmiete, die Zahl der Mitbewohner und die Beheizungsart sowie freiwillig Angaben zum Vermieter), so dass eine erneute Datenerhebung nicht erforderlich ist. Hinsichtlich der übrigen in der Mietbescheinigung erbetenen Informationen wie z.B. zu einer möglichen zusätzlichen Nutzung des Wohnraums, zur Höhe der Gesamtmiete und deren einzelnen Bestandteile sowie zu einer eventuellen öffentlichen Förderung der Wohnung ist eine regelmäßige Datenerhebung für die Entscheidung über einen Leistungsantrag ebenfalls nicht erforderlich. Darüber hinaus steht eine Datenerhebung bei dem Vermieter in Widerspruch zu dem Grundsatz der Direkterhebung (§ 67a Abs. 2 Satz 1 SGB X). Der auf den Vordrucken häufig enthaltene Hinweis, der Vermieter sei nach § 60 SGB II zur Auskunft verpflichtet, ist unzutreffend.

– Vorlage von Kontoauszügen

Zur Frage der datenschutzrechtlichen Zulässigkeit der Anforderung von Kontoauszügen durch Sozialbehörden im Zusammenhang mit einem Leistungsantrag hat der LfD in der Vergangenheit die Auffassung vertreten, dass bei einem Erstantrag auf Sozialhilfe die behördliche Bitte um Vorlage von Kontoauszügen der dem Antrag vorangegangenen drei bis sechs Monate von den Mitwirkungspflichten des Antragstellers (§§ 60 ff. SGB I) gedeckt sei (18. Tb., Tz. 11.6.3). Diese Rechtsauffassung hält der LfD angesichts der mit der Gewährung von Sozialhilfe vergleichbaren Sachlage auch im Rahmen eines Antrags auf Gewährung von Arbeitslosengeld II aufrecht. Denn zur Feststellung der Hilfebedürftigkeit des Antragstellers i.S.v. § 9 Abs. 1 SGB II stellen die Kontoauszüge der letzten drei bis sechs Monate vor der Antragstellung geeignete und erforderliche Beweismittel dar, zu deren Vorlage der Antragsteller nach behördlicher Anforderung gemäß § 60 Abs. 1 Satz 1 Nr. 3 SGB I auch verpflichtet ist. Insoweit haben die Sozialgerichte München und Dresden zu Recht darauf hingewiesen, dass für die Feststellung, ob Einkommen und Vermögen vorhanden ist, der aktuelle Kontoauszug nicht ausreiche, da die Prüfung der Kontenbewegungen der letzten Monate zur vollständigen Ermittlung der Einkommens- und Vermögenssituation des Betroffenen erforderlich sei. Die Anforderung der Kontoauszüge der letzten Monate beeinträchtige das Recht auf informationelle Selbstbestimmung nicht (Sozialgericht München, Urteil vom 9.9.2005, Az. S 50 AS 472/05 ER; Sozialgericht Dresden, Beschluss vom 1.3.2006, Az. S 34 AS 274/06).

Diese Rechtsauffassung wird im Kreise der Datenschutzbeauftragten des Bundes und der Länder überwiegend geteilt. Der LfD widerspricht ausdrücklich der von dem Hessischen Landessozialgericht getroffenen Entscheidung vom 22.8.2005 (Az. L 7 AS 32/05 ER) im Hinblick auf die dort enthaltenen Ausführungen zur Erforderlichkeit der Vorlage zurückliegender Kontoauszüge. Das Gericht hatte eine behördliche Befugnis zur Anforderung von Kontoauszügen im Zusammenhang mit der Entscheidung über Anträge auf Gewährung von Arbeitslosengeld II im Regelfall verneint. Derartige Dokumente müssten nur dann vorgelegt werden, wenn im Einzelfall tatsächlich Anhaltspunkte für einen möglichen Leistungsmissbrauch bestehen.

Im Hinblick auf die Anforderung von Kontoauszügen bei einem Folgeantrag auf Weitergewährung des Arbeitslosengeldes II hält der LfD im Regelfall eine erneute Vorlage von Unterlagen frühestens nach Ablauf von 12 Monaten für zulässig. Denn ohne weitere Anhaltspunkte für eine Änderung der bereits im Vorantrag dargelegten Einkommens- und Vermögensverhältnisse ist eine frühere Vorlage von Kontoauszügen zur Überprüfung der Voraussetzungen für eine Weiterbewilligung der beantragten Leistung regelmäßig nicht erforderlich. Bei Beachtung dieser Vorgaben ist darüber hinaus die Anforderung von Auszügen der letzten drei Monate grundsätzlich ausreichend, es sei denn, im Einzelfall wäre aufgrund konkreter Anhaltspunkte eine Vorlage von weiteren Kontoauszügen geboten.

– Errichtung eines Außendienstes/Durchführung von Hausbesuchen

Mit dem Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende wurde in § 6 Abs. 1 Satz 2 SGB II die an die Leistungsträger gerichtete Empfehlung aufgenommen, zur Bekämpfung des Leistungsmissbrauchs einen Außendienst zu errichten. Damit hat der Gesetzgeber eine bereits im Zusammenhang mit der Gewährung von Sozialhilfeleistungen bestehende Praxis der Leistungsträger aufgegriffen und gesetzlich verankert.

Aus der Sicht des Datenschutzes ist die Errichtung eines derartigen Außendienstes und die Durchführung von Hausbesuchen nicht per se ausgeschlossen. Allerdings stellt ein im Zusammenhang mit der Bewilligung von Sozialleistungen stehender Hausbesuch angesichts der Mitwirkungspflichten des Antragstellers faktisch eine Einschränkung des in Art. 13 GG enthaltenen Grundrechts auf Unverletzlichkeit der Wohnung und damit in besonderem Maße auch des informationellen Selbstbestimmungsrechts dar. Eine derartige Maßnahme ist daher nur in Ausnahmefällen unter Einhaltung der Grundsätze

der Erforderlichkeit und Verhältnismäßigkeit zulässig. Der LfD hat sich bereits in der Vergangenheit ausführlich mit der Thematik beschäftigt (vgl. 17. Tb., Tz. 11.2.6 und 18. Tb., Tz. 11.6.2). Die darin formulierten Anforderungen an einen datenschutzgerechten Einsatz von Sozialhilfeermittlern gelten auch für die Nutzung des in § 6 Abs. 2 SGB II empfohlenen Außendienstes. Der Erlass einer Dienstanweisung ist zur Gewährung einer einheitlichen und rechtskonformen Vorgehensweise geboten (vgl. hierzu z.B. die Hinweise des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zur datenschutzgerechten Ausgestaltung von Hausbesuchen einschließlich der Bereitstellung einer Musterdienstanweisung und weiterer Texte [https://www.datenschutzzentrum.de/sozialdatenschutz/hausbesuche.htm] und die seitens der BA in diesem Zusammenhang ausgearbeiteten Empfehlungen [http://www.arbeitsagentur.de/zentraler-Content/A01-Allgemein-Info/A015-Oeffentlichkeitsarbeit/Publikation/pdf/Gesetzestext-6-SGB-II-Traeger-Grundsicherung.pdf]).

Im Rahmen einer Eingabe hatte der LfD zudem die Frage zu beantworten, ob bei der Durchführung eines Hausbesuchs auch ein Praktikant den Außendienstmitarbeiter begleiten durfte. Im Ergebnis empfahl der LfD, angesichts der besonderen Schutzbedürftigkeit der verarbeiteten Daten und der geringen Verweildauer kurzzeitig in der Verwaltung tätiger Personen wie z.B. Praktikanten diesen einen Zugang zu derartigen Informationen regelmäßig nicht zu gewähren. Denn anders als die Mitarbeiter der öffentlichen Stellen, die sowohl dienst- als auch datenschutzrechtlich (§ 8 LDSG) konkreten Geheimhaltungspflichten unterliegen, ist dies bei diesem Personenkreis mangels eines bestehenden Beschäftigungsverhältnisses zunächst nicht der Fall. Zwar können im Wege einer Verpflichtung nach dem Verpflichtungsgesetz Maßnahmen gegen eine unbefugte Weitergabe der dienstlich zur Kenntnis genommenen personenbezogenen Daten getroffen werden. Es sollte jedoch die besondere Schutzbedürftigkeit der im Rahmen eines Hausbesuchs verarbeiteten Daten sowie das in § 6 SGB XII enthaltene und auf alle Sozialleistungen anwendbare Qualifizierungsgebot der in diesem Zusammenhang eingesetzten Beschäftigten beachtet werden. Eine Einbindung der o.g. Personen in eine Außendienstmaßnahme ist aus der Sicht des LfD daher nur in Ausnahmefällen zulässig.

– Verfahren A2LL
Die in Rheinland-Pfalz gebildeten ARGEn nutzen das von der BA zentral zur Verfügung gestellte Datenerhebungs- und Leistungsberechnungsprogramm A2LL. Dieses weist erhebliche datenschutzrechtliche Mängel auf. Insbesondere das fehlende Zugriffsrechte- und Löschkonzept, die generell nutzbare bundesweite Personensuche („zPDV“) mit den daraus resultierenden Zugriffsmöglichkeiten und die fehlende Protokollierung dieser lesenden Zugriffe begegnen gravierenden datenschutzrechtlichen Bedenken und wurden bereits seitens des BfDI gegenüber der BA förmlich beanstandet (vgl. 20. Tb. des BfDI, Tz. 16.1.3).

Im Rahmen der Kontrollen zur Nutzung des Verfahrens A2LL in den rheinland-pfälzischen ARGEn hat sich ergeben, dass die beanstandeten Mängel weiterhin bestanden. Der LfD hat sich der Bewertung des BfDI angeschlossen. Angesichts der Tatsache, dass das Verfahren zentral von der BA entwickelt und den ARGEn zur Verfügung gestellt wird, hat er die betroffenen ARGEn gebeten, die BA von der datenschutzrechtlichen Bewertung des LfD zu unterrichten und mitzuteilen, bis wann mit einer Behebung der datenschutzrechtlichen Mängel des Verfahrens gerechnet werden kann. Zwischenzeitlich wurde das Verfahren A2LL um die ausstehenden Funktionen für die Vergabe abgestufter Zugriffsberechtigungen und die Protokollierung bundesweiter Zugriffe ergänzt. Damit ist sichergestellt, dass die Mitarbeiter der BA nur auf die Daten zugreifen können, die für die jeweilige Sachbearbeitung erforderlich sind. Zudem sind bundesweite Zugriffe nunmehr nachvollziehbar.

Für die ARGEn kommt es nun darauf an, dass die Zugriffsrechte der Beschäftigten im erforderlichen Umfang angepasst werden. Der LfD wird dies im Rahmen seiner weiteren Kontrollen überprüfen.

11.1.4 Datenschutz bei der Gewährung von Leistungen zur Eingliederung in Arbeit; Verfahren VAM/Verbis

Die ARGEn in Rheinland-Pfalz setzen seit dem Jahr 2007 das von der BA bereitgestellte Verfahren VAM/VERBIS ein; dieses dient der Vermittlung Arbeitsuchender „Virtueller Arbeitsmarkt“ und löst die bisherigen Verfahren COMPAS und CoArb ab. Im Blickpunkt entsprechender Kontrollen des LfD stand u.a. die Frage, in welchem Umfang über VERBIS Abfrage- und Auswertungsmöglichkeiten zur Verfügung stehen und inwieweit diese in eine geeignete Umsetzung des Berechtigungskonzepts vor Ort sowie angemessene Protokollierungen eingebettet sind.

Dabei hat sich ergeben, dass ähnlich wie im Verfahren A2LL (vgl. Tz. 11.1.3) bundesweite Such- bzw. Zugriffsmöglichkeiten bestehen, ohne dass entsprechende Zugriffe gegenwärtig jedoch protokolliert werden. Die Nachvollziehbarkeit entsprechender Abfragen ist damit zurzeit nicht gegeben. Soweit den ARGEn Möglichkeiten zur Verfügung standen, Zugriffsrechte auf die konkreten Anforderungen hin zu beschränken, waren diese nicht bekannt bzw. wurden nicht genutzt. Zumeist wurde die von der Bundesagentur für Arbeit erstellte Grundkonfiguration übernommen.

Mit Blick auf die Tatsache, dass es sich bei VAM/VERBIS um ein zentrales Verfahren der Bundesagentur handelt, wurde diese in Zusammenarbeit mit dem BfDI um Klärung der genannten Punkte gebeten. Danach ist vorgesehen, im Jahr 2008 das Verfahren um entsprechende Protokollierungsfunktionen zu erweitern. Für die Auswertung von Zugriffen rheinland-pfälzischer Stellen wurde ein Verfahren vorgesehen, nach dem die Protokolldaten im konkreten Prüfungsfall von der BA bereit gestellt werden. Inwieweit dies, nicht zuletzt mit Blick auf die vorgesehene Speicherungsdauer der Protokolle für drei Monate, geeignet ist, eine angemessene Nachvollziehbarkeit zu gewährleisten, wird der LfD im weiteren Verlauf überprüfen.

Ähnliches gilt für die Vergabe der Zugriffsberechtigungen im Bereich der ARGEn. Nach Auskunft der BA gilt angesichts der uneinheitlichen Aufbau- und Ablauforganisation in den ARGEn der Grundsatz, die zur Aufgabenwahrnehmung erforderlichen Zugriffsrechte in Verantwortung der lokalen Geschäftsführung der ARGEn festzulegen. Eine pauschale Übernahme der Grundkonfiguration der BA ohne Prüfung der tatsächlichen Erfordernisse vor Ort scheidet damit im Regelfall aus; dies gilt insbesondere für den bundesweiten Zugriff auf die Daten der Stellenbewerber sowie den Zugriff der BA auf Datensätze, die der ausschließlichen Bearbeitung durch die ARGEn unterliegen.

11.2 Entwurf eines Kinderschutzgesetzes

Vor dem Hintergrund der jüngsten Fälle von Kindesmisshandlungen wurde in der Öffentlichkeit über Möglichkeiten diskutiert, Kindeswohlgefährdungen künftig frühzeitiger erkennen zu können. Nach den Vorstellungen der Landesregierung soll eine „Erhöhung der Verbindlichkeit“ kindlicher Vorsorgeuntersuchungen hier Verbesserungen bringen. Ein entsprechender Gesetzesentwurf wurde mittlerweile der Öffentlichkeit vorgestellt. Konkret geht es darum, diejenigen Eltern, die ihre Kinder nicht zur Vorsorgeuntersuchung bringen, einer „besonderen Behandlung“ zu unterziehen, ohne dabei das Prinzip der freiwilligen Inanspruchnahme aufzugeben. Um dies zu erreichen, sind komplexe Informationsvorgänge (Abgleiche, Übermittlungen und Rückmeldungen) zwischen dem Meldeamt, der beim Landesamt für Soziales, Jugend und Versorgung einzurichtenden „Zentralen Stelle“, den Kinderärzten, dem Gesundheitsamt sowie dem Jugendamt erforderlich.

Es versteht sich von selbst, dass die beabsichtigte Vorgehensweise mit einem tiefgreifenden Eingriff in das informationelle Selbstbestimmungsrecht der Sorgeberechtigten verbunden ist. Die Eltern, die – aus welchen Gründen auch immer – das Angebot der Vorsorgeuntersuchung nicht wahrnehmen möchten, sehen sich zunächst einmal dem Generalverdacht ausgesetzt, ihr Kind zu vernachlässigen oder gar zu misshandeln.

Der LfD hat sich daher frühzeitig in das Gesetzgebungsverfahren eingebracht. Im Rahmen einer Expertenanhörung vor dem Sozialpolitischen Ausschuss des Landtags hatte er Gelegenheit, die datenschutzrechtlichen Anforderungen, die an ein solches Gesetz zu stellen sind, vorzutragen. Hieran anschließend fand ein intensiver Informationsaustausch mit dem MASGFF statt. Zahlreiche Verbesserungsvorschläge des LfD konnten dadurch berücksichtigt werden:

Insbesondere wurde erreicht, dass die Datenflüsse normenklar geregelt und Daten von Nichtteilnehmern, bei denen es keine Anzeichen für eine Kindeswohlgefährdung gibt, zeitnah aus den Behördenakten entfernt werden. Herauszuheben ist die auf Vorschlag des LfD aufgenommene Evaluation in Bezug auf die Wirksamkeit des neuen Verfahrens. Es entspricht nämlich einem grundsätzlichen Anliegen des Datenschutzes, dass Gesetze, die in das Selbstbestimmungsrecht einer Vielzahl von Personen eingreifen, rückblickend bewertet und einer kritischen Prüfung unterzogen werden können. Ob sich daraus für den Bereich des Datenschutzes Handlungsbedarf ergeben wird, ist derzeit noch nicht absehbar. So muss sichergestellt werden, dass die handelnden Behörden über die erforderlichen Sach- und Personalmittel verfügen, um einerseits unauffällig gewordene Datensätze zeitnah zu löschen und andererseits auffällig gewordene Datenbestände unverzüglich zu überprüfen.

Innerhalb des Berichtszeitraums konnte die Frage, ob und inwiefern die Aufgaben der „Zentralen Stelle“ auch von einer Stelle außerhalb des Landes wahrgenommen werden können, nicht abschließend geklärt werden. Datenschutzrechtlich geht es dabei um die Frage, ob lediglich eine Auftragsdatenverarbeitung vorliegt oder von einer weiter gehenden Funktionsübertragung auszugehen ist. Letztere wäre nur auf der Basis einer Rechtsgrundlage zulässig. Von daher wird auch weiterhin eine intensive Befassung mit der Thematik erforderlich sein.

11.3 oscare – eine neue Software für die Allgemeinen Ortskrankenkassen

Im Oktober 2006 hat der LfD die Leitung der von den Datenschutzbeauftragten des Bundes und der Länder eingerichteten Arbeitsgruppe zur neuen AOK-Software oscare übernommen. Die Arbeitsgruppe begleitet schon seit einigen Jahren aus der Sicht des Datenschutzes die Entwicklung des früher unter dem Namen „AOK-SAM“ bezeichneten Verfahrens, das künftig das veraltete EDV-System IDVS II vollständig ablösen soll. Dieser Prozess ist in drei große Entwicklungsprojekte gegliedert: Firmenkundenservice, Leistungswesen und Bestandsführung, wobei die Pilotierung der für das Leistungswesen entwickelten Programmanwendung von oscare bei der AOK Rheinland-Pfalz erfolgte. Zielsetzung der an der Verfahrensentwicklung

beteiligten Organisationen – neben dem AOK-Bundesverband und einigen Landeskassen sind dies die AOK-Systems und die SAP AG – ist die Schaffung einer über den AOK-Verbund hinausgehenden Standardsoftware in der gesetzlichen Krankenversicherung.

Die Arbeitsgruppe der Datenschutzbeauftragten hat sich in der Vergangenheit im Schwerpunkt mit datenschutzrechtlichen Fragestellungen befasst, die sich bereits auf einer übergeordneten Ebene der neuen Software, der sog. Masterebene, lösen lassen. Hierzu gehören u.a.:

- die grundsätzliche Ausgestaltung von Rollen und Berechtigungen einschließlich der Möglichkeit, diese regional zu beschränken,
- der Einsatz von Mechanismen zur Protokollierung von aus der Sicht des Datenschutzes sensiblen Datenverarbeitungen,
- die Formulierung von Standardvorgaben zur Archivierung und Löschung der gespeicherten Sozialdaten,
- Art und Umfang der über ein Business Warehouse bereit gestellten personenbezogenen Auswertungsmöglichkeiten sowie
- die Implementierung prüfungsunterstützender Funktionen zur effektiven Durchführung von Datenschutzkontrollen.

Das Engagement der Arbeitsgruppe hat sich aus der Sicht des Datenschutzes bislang durchaus gelohnt. So konnte beispielsweise verhindert werden, mit der neuen Software einen versichertenbezogenen Deckungsbeitragswert („Scorewert“) zu errechnen. Weiterhin wurde die Vorlage von Standardvorgaben zur Archivierung und Löschung der verarbeiteten Daten zugesagt und die Bereitstellung prüfungsunterstützender Funktionen in Aussicht gestellt. Ungeachtet des bereits Erreichten wird die Arbeitsgruppe bei den noch offenen wie auch bei künftigen Themenfeldern versuchen, bei der Weiterentwicklung der Software die Belange des Datenschutzes angemessen zu berücksichtigen. Die bisher äußerst konstruktive Zusammenarbeit mit dem oscare-Management bietet hierfür eine gute Ausgangsbasis.

11.4 Anforderung ärztlicher Unterlagen auf der Basis des § 294a SGB V

Im Berichtszeitraum ist der LfD wiederholt um Prüfung gebeten worden, unter welchen Voraussetzungen Krankenkassen auf der Grundlage des § 294a SGB V ärztliche Unterlagen von Leistungserbringern anfordern dürfen. Nach Erörterung der Thematik im Kreise der Datenschutzbeauftragten des Bundes und der Länder vertritt der LfD hierzu folgende Rechtsauffassung:

- § 294a Satz 1 SGB V stellt eine gesetzliche Verpflichtung der darin genannten Leistungserbringer dar, den Krankenkassen die zur Klärung möglicherweise bestehender Ersatz- oder Erstattungsansprüche erforderlichen Daten mitzuteilen. Soweit die betroffenen Daten der ärztlichen Schweigepflicht unterliegen, beinhaltet § 294a Satz 1 SGB V zugleich eine gesetzliche Befugnis zur Offenbarung dieser Daten, so dass die Einholung einer Schweigepflichtentbindungserklärung bei dem Versicherten in diesem Zusammenhang entbehrlich ist.
- Bei Vorliegen der Voraussetzungen des § 294a Satz 1 SGB V steht der betroffenen Krankenkasse ein Rechtsanspruch gegen den Leistungserbringer auf Übermittlung der erforderlichen Daten zu.
- § 294a Satz 1 SGB V berechtigt die betroffene Krankenkasse nicht, gegenüber einem Leistungserbringer Ermittlungen ins Blaue hinein durchzuführen. Vielmehr bedarf es des Vorliegens konkreter Anhaltspunkte bzw. Hinweise i.S.v. § 294a Satz 1 SGB V für einen der dort genannten Tatbestandsalternativen. Soweit sich eine Krankenkasse bei der Anforderung von Daten bei einem Leistungserbringer auf § 294a SGB V beruft, muss sie daher die im zugrunde liegenden Fall aus ihrer Sicht bestehenden Anhaltspunkte oder Hinweise i.S.v. § 294a Satz 1 SGB V zumindest ansatzweise bezeichnen. Allgemeine oder pauschale Formulierungen ohne konkrete Bezugnahme auf die Gegebenheiten im Einzelfall und die daraus resultierende Vermutung eines möglicherweise bestehenden Ersatz- oder Erstattungsanspruchs reichen hierzu grundsätzlich nicht aus.
- Der Rechtsanspruch aus § 294a Satz 1 SGB V umfasst lediglich die Daten, die zur Klärung der von der Krankenkasse dargelegten Vermutung eventuell bestehender Regressforderungen erforderlich sind. Die restriktiv auszulegende Regelung des § 294a Satz 1 SGB V schließt die Bereitstellung kompletter Krankenakten regelmäßig aus. Soweit möglich soll die Krankenkasse die von ihr unter Bezugnahme auf § 294a SGB V erbetenen Unterlagen und Informationen konkret bezeichnen, um die Übermittlung nicht erforderlicher Daten auszuschließen.

Maßgeblich für die Frage der Erforderlichkeit der angeforderten Informationen sind die Umstände des Einzelfalls. Im Rahmen der Erforderlichkeitsprüfung sollte die Krankenkasse unter Berücksichtigung der bei ihr schon vorhandenen Informationen (z.B. Daten nach § 301 SGB V) dem Leistungserbringer die im jeweiligen Fall zur Klärung benötigten Angaben beschreiben.

11.5 Anforderung von Arztberichten zur Genehmigung pädagogischer Frühfördermaßnahmen durch einzelne Jugendämter

Durch einen Hinweis aus der Ärzteschaft wurde dem LfD bekannt, dass einzelne Jugendämter im Zusammenhang mit der Gewährung von Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche nach § 35a SGB VIII von den Antragstellern

regelmäßig die Vorlage eines Arztberichts oder die Abgabe von Einwilligungs- und Schweigepflichtentbindungserklärungen verlangen. Nach Auffassung der betroffenen Ärzte war eine derart weitreichende Datenerhebung im Regelfall jedoch nicht erforderlich, da den Jugendämtern zur Genehmigung der Leistungsanträge ein ärztlicher Förderplan, der sowohl eine Dokumentation der diagnostischen Maßnahmen als auch der Therapieempfehlungen beinhaltet, zur Verfügung gestellt werde. Damit sei den Anforderungen des § 35a Abs. 1a Satz 1 SGB VIII, der die Einholung einer fachärztlichen Stellungnahme verlange, ausreichend entsprochen. Die Arztberichte dienten dagegen ausschließlich der Kommunikation zwischen den beteiligten Medizinern.

Auch nach Auffassung des von dem konkreten Hinweis betroffenen Jugendamtes hat sich die Datenerhebung im Zusammenhang mit § 35a Abs. 1a Satz 1 SGB VIII auf den hierfür erforderlichen Umfang zu beschränken. Vor diesem Hintergrund kündigte das Jugendamt an, künftig auf die zusätzliche Anforderung ärztlicher Unterlagen mittels einer Einwilligungserklärung zu verzichten. Denn bei Antragstellung seien den Antragsunterlagen regelmäßig die zur Beurteilung erforderlichen Daten beigefügt. Sollte in Ausnahmefällen noch Klärungsbedarf bestehen, sei hierzu ein persönliches Gespräch mit den Beteiligten vorgesehen. Im Ergebnis stellt dies eine deutliche Stärkung des Datenschutzes dar.

11.6 Datenverarbeitung im Zusammenhang mit der Prüfung des Nachrangs der Sozialhilfe

Zu einer formellen Beanstandung des betreffenden Sozialamtes wegen Verletzung des Sozialgeheimnisses führte folgender Sachverhalt:

Im Zusammenhang mit der Beantragung von Leistungen der Eingliederungshilfe nach den §§ 53 ff. SGB XII erklärte eine Antragstellerin auf einem Formularblatt ihr Einverständnis, dass in der Hilfeplankonferenz (HPK) der Leistungsträger ihr Antrag namentlich besprochen und ihre personenbezogenen Daten an die Teilnehmer der Konferenz weitergegeben werden. Zugleich unterzeichnete sie eine formularmäßig vorbereitete Erklärung zur Entbindung von der ärztlichen Schweigepflicht und zum Datenschutz. Der Petentin wurden nach Durchführung der HPK und Feststellung des Hilfebedarfs Leistungen der Eingliederungshilfe in Form eines persönlichen Budgets bewilligt. Darauf hin wurde die Petentin von einer von ihr ausgesuchten Integrationshelferin betreut. Auf Grund der bei der Antragstellung erhobenen ärztlichen Diagnose, die an die Teilnehmer der HPK weitergegeben worden war, lagen nach Darstellung des zuständigen Sozialamtes Hinweise für eine Gewalterfahrung der Petentin vor (Drittverschulden/möglicher Missbrauch). Nach Auffassung des Sozialamtes ergab sich deshalb die Notwendigkeit, einen eventuellen Nachrang der Sozialhilfe (z.B. gegenüber Ansprüchen nach dem Opferentschädigungsrecht/§ 116 SGB X) zu überprüfen.

Im Rahmen des weiteren Vorgehens sah das Sozialamt zum vermeintlichen Wohle der Petentin davon ab, diese selbst mit der Missbrauchsvermutung zu konfrontieren. Vielmehr beabsichtigte man, zunächst weitere Informationen bei Dritten zu sammeln, die den Verdacht einer drittschädigenden Handlung erhärteten. Das Sozialamt wandte sich daher u.a. an die Integrationshelferin der Petentin mit der Bitte um Informationen zu der aus der Sicht der Behörde bestehenden Missbrauchsvermutung. Eine Unterrichtung der Petentin war nicht beabsichtigt. Sie erfuhr vielmehr erst durch ihre Integrationshelferin von dem Vorgehen des Sozialamtes. Nach ihrer Darstellung hätte sie diesem ohne Weiteres auf Nachfrage mitteilen können, dass in einem von ihr selbst angestrengten gerichtlichen Verfahren eventuelle Ansprüche nach dem OEG bereits rechtskräftig abgelehnt worden waren.

Nach Auffassung des LfD stand die Beschaffung weitergehender, einen möglichen Missbrauch der Petentin betreffenden Informationen bei Dritten im Widerspruch zu den sozialdatenschutzrechtlichen Vorgaben. Denn nach § 67a Abs. 2 Satz 1 SGB X sind Sozialdaten im Regelfall bei dem Betroffenen selbst zu erheben. Angesichts der mit einer Datenerhebung bei Dritten zwangsläufig verbundenen Informationsweitergabe lässt der Gesetzgeber eine von dem Direkterhebungsgrundsatz abweichende Dritterhebung nur ausnahmsweise und unter sehr engen Voraussetzungen zu. Eine Datenerhebung bei Dritten ist regelmäßig unzulässig, wenn Anhaltspunkte für eine damit einhergehenden Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen bestehen. Dies war der Fall, da im Rahmen der Informationsbeschaffung bei der Integrationshelferin besonders sensible Angaben über die Petentin übermittelt wurden. Zugleich lagen keine konkreten Anhaltspunkte für die Annahme vor, dass die Konfrontation der Betroffenen mit der Missbrauchsvermutung zu einer Beeinträchtigung schutzwürdiger Interessen wie z.B. einer erheblichen Gesundheitsgefährdung geführt hätten. Im konkreten Fall hätte es insoweit nahe gelegen, erforderliche Ermittlungen im Hinblick auf die Missbrauchsvermutung durch Befragung der Petentin selbst durchzuführen und darauf zu verzichten, anderen Personen bzw. Stellen im Rahmen der Informationsbeschaffung diese sensiblen Angaben zu offenbaren. Die bisherige Verwaltungspraxis des Sozialamts, aus Gründen der Fürsorge den Betroffenen im Zweifel nicht an der Feststellung möglicher Ansprüche gegenüber Dritten zu beteiligen, wich dagegen in erheblichem Maße von der gesetzlichen Wertung ab.

Das Sozialamt versicherte die zukünftige Einhaltung der datenschutzrechtlichen Vorgaben.

11.7 Bildungs- und Lerndokumentationen in Kindertagesstätten

Im 20 Tb. wurde von der Novellierung des Kindertagesstättengesetzes und der damit im Zusammenhang stehenden Einführung von Bildungs- und Lerndokumentationen berichtet (Tz. 11.8). Da die datenschutzrechtlichen Anforderungen, die an das Führen dieser „kindlichen Akte“ zu stellen sind, im Gesetz nicht geregelt wurden, hatte der LfD gefordert, dies in einer Handreichung für die Kindertagesstätten nachzuholen. Der Landesjugendhilfeausschuss nahm sich der Sache an und beauftragte eine Arbeitsgruppe, an der auch Vertreter des LfD, des Bildungsministeriums sowie der Kirchen beteiligt waren, einen entsprechenden Text zu erstellen. Da die redaktionellen Arbeiten im Berichtszeitraum noch nicht abgeschlossen waren, ist eine Veröffentlichung des vollständigen Textes im Rahmen des Tätigkeitsberichtes leider nicht möglich. Gegenstand der Handreichung sind aber die nachfolgend abgedruckten zehn Regeln zum datenschutzgerechten Umgang mit Bildungs- und Lerndokumentationen (A) sowie die insoweit zu beachtenden technisch-organisatorischen Anforderungen (B).

A) 10 Regeln zum datenschutzgerechten Umgang mit Bildungs- und Lerndokumentationen in Kindertagesstätten

1. Das Führen der Bildungs- und Lerndokumentation ist gesetzlich geregelt (§ 2 KitaG) und bedarf insoweit nicht der Einwilligungserklärung der Erziehungsberechtigten.
2. Die Erziehungsberechtigten sind aber darüber zu unterrichten, dass
   a) eine Bildungs- und Lerndokumentation über ihr Kind angelegt wird und
   b) ihnen ein Akteneinsichtsrecht zusteht.
3. Es dürfen nur solche Informationen aufgenommen werden, die für die Aufgabenerfüllung der Kita notwendig sind (Grundsatz der Erforderlichkeit); bei der Erhebung besonders schützenswerter Daten (z.B. Gesundheitsdaten, Daten über Religion, ethnische Herkunft, defizitorientierte Erhebungen) ist ein besonders strenger Maßstab anzulegen.
4. Bevor die Dokumentation angelegt wird, sollte geprüft werden, ob und inwiefern eine namentliche Nennung des betroffenen Kindes und von Spielkameraden erforderlich ist. Denkbar ist beispielsweise ein Verfahren, bei dem der Name des Kindes nur auf dem Deckblatt erscheint, ansonsten jedoch eine Abkürzung (z.B. erster Anfangsbuchstabe des Vornamens) verwendet wird.
5. Die Weitergabe der Bildungs- und Lerndokumentation ist ohne schriftliche Einwilligungserklärung der Erziehungsberechtigten nicht zulässig; dies gilt auch für Anfragen von Grundschulen.
6. Die Einwilligung muss so konkret wie möglich formuliert werden (welche Daten sollen an welche Personen oder Stellen zu welchem Zweck weitergegeben werden?). Auf lediglich pauschale Erklärungen, die z.B. bei Aufnahme des Kindes eingeholt werden, kann eine Informationsweitergabe nicht gestützt werden.
7. Verlässt das Kind die Kita, ist die Bildungs- und Lerndokumentation entweder an die Erziehungsberechtigten herauszugeben oder zu vernichten.
8. Die weitere Aufbewahrung für interne Qualitätssicherungszwecke ist zulässig, wenn die Daten anonymisiert wurden. Werden Bildungs- und Lerndokumentationen für Zwecke der wissenschaftlichen Forschung angefordert, sollte ebenfalls eine vorherige Anonymisierung erfolgen.
9. Bildungs- und Lerndokumentationen sind vor unbefugter Kenntnisnahme zu schützen.
10. In Zweifelsfragen Kontakt zu den Aufsichtsbehörden aufnehmen (Übersicht unter http://www.datenschutz.rlp.de/):
    a) Für Kitas in kirchlicher Trägerschaft: Kirchliche Datenschutzbeauftragte;
    b) für Kitas in öffentlicher Trägerschaft: Der Landesbeauftragte für den Datenschutz
    c) für Kitas in privater Trägerschaft: die Aufsichts- und Dienstleistungsdirektion Trier (ADD).

B) Technisch-organisatorische Datenschutzfragen im Zusammenhang mit Bildungs- und Lerndokumentationen

Aufgrund der besonderen Gefahren, die mit der automatisierten Datenverarbeitung einhergehen, hat das Bundesverfassungsgericht in seinem Volkszählungsurteil gefordert, dass der Gesetzgeber insoweit organisatorische und verfahrensrechtliche Regelungen zu treffen habe. Die automatisierte Datenverarbeitung sollte jedoch nicht nur als Risiko, sondern auch als Chance betrachtet werden: Die Vergabe differenzierter Zugriffsberechtigungen oder die Gewährleistung einer zeitgerechten Löschung ist beispielsweise im automatisierten Verfahren wesentlich einfacher umzusetzen, als dies bei der herkömmlichen Verarbeitung in Akten oder auf Karteikarten der Fall ist. Soweit die technisch-organisatorischen Vorgaben Beachtung finden, ist daher keine der genannten Verarbeitungsformen aus Sicht des Datenschutzes besonders vorzugswürdig.

Vorschriften zum technisch-organisatorischen Datenschutz finden sich – je nach Trägerschaft der Kindertagesstätte – in § 9 LDSG, § 9 BDSG, § 78a SGB X und in den einschlägigen kirchlichen Datenschutzregeln. Diese beinhalten primär Bestimmungen, die bei der automatisierten Datenverarbeitung zu beachten sind. Aber auch bei der Verarbeitung

personenbezogener Daten im nicht-automatisierten Verfahren sind Maßnahmen zu treffen, die insbesondere eine Kenntnisnahme von Unbefugten verhindern.

Bezogen auf die Besonderheiten der jeweiligen Stelle sind die technisch-organisatorischen Datenschutzmaßnahmen in einer internen Dienstanweisung im Einzelnen niederzulegen. Ein Muster für die Dienstanweisung findet sich unter http://www.datenschutz.rlp.de/ (Rubrik „Materialien zum Datenschutz“; „Hinweise und Empfehlungen“; „Regelungsbeispiele für eine Musterdienstanweisung“). Auch Löschfristen sollten hierin aufgenommen werden. Sind keine gesetzlich festgelegten Fristen vorhanden, hat die verantwortliche Stelle die Speicherfristen selbst in einer Dienstanweisung festzulegen. Die Dauer der Aufbewahrung hat sich dabei am Erforderlichkeitsgrundsatz zu orientieren.

Was die Bildungs- und Lerndokumentation angeht, sollte klar geregelt werden, dass diese bei Verlassen der Einrichtung entweder gelöscht oder den Erziehungsberechtigten ausgehändigt wird. Sofern die Nutzung der Dokumentation für Qualitätssicherungszwecke beabsichtigt ist, sollte eine vorherige Anonymisierung vorgeschrieben werden.

Nachfolgend einige Beispiele, wie dem technisch-organisatorischem Datenschutz bei der Verarbeitung von personenbezogenen Daten im nicht-automatisierten Verfahren und im automatisierten Verfahren Rechnung getragen werden kann:

a) Datenschutz bei der nicht-automatisierten Verarbeitung von Daten

   Schon bei der Erhebung der Daten sollte berücksichtigt werden, dass die Dokumentationen später für Qualitätssicherungszwecke verwendet werden können. Der Name des Kindes sollte daher nur auf dem Deckblatt erscheinen, ansonsten sollte eine Abkürzung (z.B. erster Anfangsbuchstabe des Vornamens) verwendet werden. Gleiches gilt für den Fall, dass andere Kinder („Dritte“) in der Dokumentation erwähnt werden. Evtl. gefertigte Fotos sollten in der Akte separat vorgehalten werden, damit sie später leichter entnommen werden können.

   Bei der papiergebundenen Verarbeitung personenbezogener Daten ist sicherzustellen, dass Unbefugte (z.B. Besucher der Kita) die Daten von Kindern, Erziehungsberechtigten und Beschäftigten der Kita nicht zur Kenntnis nehmen können. Bildungs- und Lerndokumentationen sollten daher nicht offen herumliegen, sondern in verschlossenen Behältnissen, im Bereich der jeweiligen Gruppe oder im Büro des Leiters aufbewahrt werden.

   Die Vernichtung von Akten oder Aktenbestandteilen sollte durch Schreddern erfolgen; notwendige Löschungen zu einem früheren Zeitpunkt durch Schwärzung. Größere Aktenmengen können auch im Wege einer Auftragsdatenverarbeitung durch einen zuverlässigen gewerblichen Anbieter entsorgt werden. Hinweise zur Vertragsgestaltung können dem Internetangebot des LfD unter der o.g. Adresse entnommen werden.

b) Datenschutz bei der automatisierten Verarbeitung von Daten

   Durch die Vergabe entsprechender Zugriffsrechte ist sicherzustellen, dass nur diejenigen Personen (lesenden/schreibenden) Zugriff auf die Bildungs- und Lerndokumentationen erhalten, die dies im Rahmen ihrer Tätigkeit benötigen. Bei Praktikanten dürfte eine diesbezügliche Notwendigkeit grundsätzlich nicht bestehen. Die Zugriffsberechtigung sollte sich an den vorhandenen Spiel- und Lerngruppen orientieren und nicht von vornherein für sämtliche Erzieherinnen und Erzieher gruppenübergreifend eingerichtet werden. Um Vertretungsregelungen abzubilden, können anlassbezogen oder dauerhaft die notwendigen Berechtigungen vergeben werden. Keine Bedenken bestehen, wenn dem Leiter der Einrichtung ein umfassendes Zugriffsrecht eingeräumt wird.

   Um die erhobenen Daten für Qualitätssicherungszwecke datenschutzgerecht nutzen zu können, muss der Personenbezug entfallen (Anonymisierung). Dies kann im Regelfall dadurch sichergestellt werden, dass die Namensangaben gelöscht werden.

   Werden auf dem Rechner darüber hinausgehend personenbezogene Daten verarbeitet (z.B. Adressaten der Erziehungsberechtigen, Protokolle von Elternausschusssitzungen, Personaldaten der Beschäftigten), muss entweder über die Vergabe von Zugriffsrechten oder durch eine Verschlüsselung der Daten eine Kenntnisnahme durch Unbefugte ausgeschlossen werden.

   Um eine angemessene Nachvollziehbarkeit der Nutzung der Bildungs- und Lerndokumentation sicherzustellen, sind insbesondere Vorgänge, wie z.B. der Ausdruck, die Übermittlung oder die Löschung von Daten zu protokollieren. Die Protokollierungspflicht erstreckt sich weiterhin auch auf die Erhebung, Speicherung, Nutzung und Sperrung personenbezogener Daten. Soweit systemseitig oder über die jeweiligen Anwendungen keine entsprechenden Protokollfunktionen zur Verfügung stehen, ist dies manuell zu dokumentieren. Als personenbezogene Daten unterliegen Protokolldaten dem Anwendungsbereich des Datenschutzrechts. Sie sollten nicht länger als ein Jahr aufbewahrt werden und dürfen nicht für Zwecke einer allgemeinen Leistungs- oder Verhaltenskontrolle verwendet werden.

   Die PC sind mit Identifikations- (z.B. Benutzerkennung) und Authentifikationsmechanismen (z.B. Passwort) abzusichern. Weitere Maßnahmen in diesem Zusammenhang sind insbesondere:

   – Dunkelschaltung des Bildschirms mit Passwortschutz bei Abwesenheit,

– Begrenzung der Fehlversuche bei der Anmeldung,
– Zeitliche Begrenzung der Gültigkeit der Passworte.

Die Räumlichkeiten, in denen PC aufgestellt werden, sollten nicht allgemein zugänglich sein, sondern bei Verlassen abgeschlossen werden.

Als Maßnahme zur Datensicherung sollte der Datenbestand regelmäßig auf separate Datenträger kopiert werden und diese an einem sicheren Ort (z.B. Tresor) aufbewahrt werden.

Soweit die eingesetzten Arbeitsplatzrechner über eine Internetanbindung verfügen, sind Vorkehrungen gegen unbefugte Zugriffe aus dem Internet (Firewall) und ein regelmäßig zu aktualisierender Schutz vor Schadsoftware (Virenschutzprogramm) vorzusehen. Entsprechende Informationen stehen z.B. unter http://www.bsi-fuer-buerger.de/ zur Verfügung).

12. Ausländerwesen

12.1 Nachweise zur Bonität des Einladers eines visapflichtigen Ausländers

Wenn Ausländer aus bestimmten Staaten, für die bei der Einreise nach Deutschland eine Visumspflicht besteht, einreisen wollen, brauchen sie häufig eine Einladung von einem Deutschen. Dieser muss sich bereit erklären, möglicherweise notwendig werdende Kosten des Aufenthalts (wie Krankheits- oder Rückführungskosten) ähnlich wie ein Bürge zu tragen. Entsprechende Verpflichtungserklärungen sind in §§ 66 bis 68 AufenthG vorgesehen.

Eine Ausländerbehörde verlangte regelmäßig zum Nachweis der Bonität die Vorlage des Mietvertrags/Wohnungsbogens (vom Vermieter ausgefüllt und unterschrieben), die Lohnabrechnungen der letzten drei Monate, die Kontoauszüge der letzten drei Monate und Nachweise über bestehende Ratenkredit- oder Darlehensverträge (diese Anforderungen fanden sich auch im Internetangebot der Behörde). Ein Betroffener ersuchte den LfD um Prüfung der Erforderlichkeit dieser Datenerhebungen. Zweifel daran ergaben sich insbesondere aus der Forderung, neben den aktuellen Lohnabrechnungen der letzten drei Monate auch Nachweise über bestehende Ratenkredit- oder Darlehensverträge und die Kontoauszüge der letzten drei Monate vorzulegen. Zwar orientieren sich die Ausländerbehörden an den vorläufigen Anwendungshinweisen des Bundesinnenministeriums, bei Detailfragen bestehen aber weiterhin Unklarheiten. Es ist derzeit nicht absehbar, wann die endgültige Fassung verbindlicher Anwendungshinweise vorliegen wird. Bis dahin konnte mit dem rheinland-pfälzischen ISM Einigkeit darüber erzielt werden, dass bei Kurzaufenthalten regelmäßig eine Glaubhaftmachung als ausreichend anzusehen ist. Bestehen allerdings Zweifel an der Kontinuität der Einkommensquelle, ist auch aus datenschutzrechtlicher Sicht gegen die Vorlage der aktuellen Verdienstbescheinigung und einer ergänzenden Vorlage entsprechender Bescheinigungen der letzten drei vorangegangenen Monate nichts einzuwenden. Das Verlangen nach der Vorlage von Kontoauszügen sollte aber in jedem Fall unterbleiben, da damit regelmäßig die Offenbarung weiterer für die Bonitätsprüfung unerheblicher Informationen verbunden ist.

Aufgrund der Intervention des LfD änderte die in Rede stehende Ausländerbehörde die Formulierung in ihrem Internetangebot ab. Nunmehr gilt die Bonität durch Vorlage der Gehaltsbescheinigung über das monatliche Nettoeinkommen als nachgewiesen. Informationsbesuche des LfD bei zwei weiteren Ausländerbehörden ergaben zunächst, dass dort die Datenerhebungen bei den Einladern auf das notwendige Maß beschränkt waren. Es fehlten allerdings Regelungen über die Löschung der in den jeweiligen elektronischen Datenverarbeitungssystemen über diese Verpflichtungen gespeicherten Daten und der Akten in Papierform. Die bei den Ausländerbehörden vorhandene Vorstellung von einer zehnjährigen Aufbewahrungszeit begegnet datenschutzrechtlichen Bedenken. Der LfD empfahl eine maximale Speicherdauer von fünf Jahren. Er wird sich darum bemühen, für diese Frage eine landesweit einheitliche Lösung zu finden.

12.2 Ausschreibungen von Ausländern zur Einreiseverweigerung im Schengener Informationssystem – SIS –

Das Schengener Informationssystem dient in erster Linie der Information der Grenzpolizeibehörden – aber auch anderer Polizeibehörden –, ob einem Ausländer die Wiedereinreise zu versagen ist oder ob nach ihm aus anderen Gründen gefahndet wird. Die nach dem Schengener Abkommen eingerichtete Gemeinsame Kontrollinstanz, deren Aufgabe die datenschutzrechtliche Überwachung dieses Informationssystems ist, hatte beim BfDI angeregt, in allen Vertragsstaaten eine koordinierte Prüfung der datenschutzrechtlichen Zulässigkeit von Ausschreibungen durchzuführen. Die Landesdatenschutzbeauftragten erklärten sich sämtlich bereit, eine solche Prüfung für ihren Bereich durchzuführen. Zu diesem Zweck hat der LfD von insgesamt 27 rheinland-pfälzischen Ausschreibungen nach Art. 99 des Schengener Durchführungsübereinkommens – SDÜ – acht Stichproben, deren Sachbearbeitung in die Zuständigkeit von vier Polizeipräsidien und dem Landeskriminalamt fielen, datenschutzrechtlich untersucht. In keinem der überprüften Fälle war dokumentiert worden, was Anlass der Ausschreibung war

(also aufgrund welcher Alternative des Artikels 99 SDÜ die Ausschreibung im SIS erfolgt war). Darüber hinaus fehlte bei Speicherungen über die Dauer eines Jahres hinaus die Dokumentation, warum eine so lange Speicherung erforderlich war. Diese Dokumentation wird ausdrücklich von Art. 112 Abs. 1 SDÜ gefordert. Der LfD empfahl nach Prüfung der jeweils beigezogenen Akten, vier Ausschreibungen zu löschen. Außerdem regte er an, verbindlich anzuordnen, dass künftig SIS-Ausschreibungen und Verlängerungen ausschließlich aufgrund einer ausdrücklichen schriftlichen Verfügung der Ausschreibungsbehörde vorgenommen werden dürfen. Das Landeskriminalamt Rheinland-Pfalz folgte den Empfehlungen des LfD.

Das Schengener Informationssystem soll zu einem erheblich leistungsfähigeren umfassenden Recherchesystem ausgebaut werden („SIS II"; s. dazu den 21. des BfDI Tz. 3.2.4.1). Die Datenschutzbeauftragten begleiten diese Entwicklung aufmerksam.

12.3 Merkblatt für Ausländerbehörden zur Erkennung islamistischer Gewalttäter

Vom BKA wurde ein Merkblatt für die Ausländerbehörden entwickelt, um diese zu veranlassen, den Polizeibehörden Verdachtsfälle von „potentiellen islamistischen Gewalttätern" zu melden. Das Innenministerium des Landes hat eine Fassung für die Landesbehörden formuliert, die mit dem LfD erörtert wurde.

Seine Bedenken richteten sich insbesondere gegen eine Formulierung, wonach sich bei Kontakten der Ausländerbehörde mit den Betroffenen „aus anfallenden Informationen ein Hinweis auf mögliche Gewalttäter ergeben" könnte, die der Polizei gemeldet werden sollen. Diese Formulierung lässt die Interpretation zu, dass die im Merkblatt angeführten Daten durch die Ausländerbehörden zielgerichtet zum Zweck der Klärung, ob ein Verdachtsfall vorliegt, erhoben werden dürften. Dies entspricht aber aus der Sicht des LfD nicht der Rechtslage, denn die Ausländerbehörden dürfen nur solche Informationen zur Grundlage ihrer Beurteilung, ob ein Verdachtsfall vorliegt, machen und ggf. an die Polizei übermitteln, die sie entweder zur Erfüllung ihrer eigenen Aufgaben rechtmäßig erhoben haben oder die ihnen ohne eigene Erhebungshandlung (zufällig) zur Kenntnis gelangt sind.

Es sollte deutlich zum Ausdruck kommen, dass der in dem Merkblatt genannte Kriterienkatalog zur Verdachtsschöpfung keine besondere Datenerhebungsbefugnis für die Ausländerbehörden begründet. Diese dürfen sich ausschließlich auf die rechtmäßig zur eigenen Aufgabenerfüllung erhobenen sowie auf die ihnen ohne Erhebungshandlung sonst (zufällig) bekannt gewordenen Informationen stützen.

Darüber hinaus vertritt der LfD die Auffassung, dass die außerhalb von Erhebungshandlungen zur Kenntnis gelangten Informationen im Verdachtsfall genutzt bzw. den Polizeibehörden übermittelt werden dürfen; diese Informationen unterliegen im vorliegenden Zusammenhang, der durch eine besondere allgemeine Gefahrenlage gekennzeichnet ist, keinem Verwertungsverbot.

12.4 Eingaben

12.4.1 Unzulässige Datennutzung bei einem anonymen Hinweis

Eine Bankbedienstete informierte von sich aus das Ausländeramt, dass ein chinesischer Student bestimmte Barabhebungen vorgenommen hätte. Das Ausländeramt nutzte diese Informationen, um die Voraussetzungen des Aufenthaltsstatus zu überprüfen. Es habe nicht wissen können, dass die anonym mitgeteilten Informationen von einer Bankbediensteten herrührten, die das Bankgeheimnis verletzt habe. Fraglich – und vom LfD zu beurteilen – war, ob diese Datennutzung zulässig war. Er ging dabei davon aus, dass sich aus den Umständen der telefonischen Informationsübermittlung für das Ausländeramt mit überwiegender Wahrscheinlichkeit ergeben hatte, dass die erlangten Informationen unter Verstoß gegen das Bankgeheimnis durch eine Bankbedienstete weitergegeben worden sind.

Der LfD hat die weitere Verwendung der aufgrund dieses Telefonats erlangten Daten wie folgt bewertet: Das Landesdatenschutzgesetz gelte neben bzw. ergänzend zu den speziellen Vorschriften der ausländerrechtlichen Gesetze für die Datenverarbeitung von rheinland-pfälzischen Ausländerbehörden. Die datenempfangende Stelle habe insbesondere dann eine Prüfpflicht, ob die Datenübermittlung rechtmäßig erfolgt sei, wenn sich Anhaltspunkte dafür aufdrängen würden (Rechtsgedanke aus § 14 Abs. 3 Satz 3 LDSG). Eine solche Verpflichtung ergibt sich zudem aus dem Rechtsstaatsprinzip des Grundgesetzes. Voraussetzung für das Speichern und Nutzen von Daten ist, dass dies für die rechtmäßige Aufgabenerfüllung der datenverarbeitenden Stelle erfolgt (§ 13 Abs. 1 Nr. 1 LDSG). Eine Aufgabenerfüllung einer öffentlichen Stelle unter Nutzung von Daten, die ihr rechtswidrig übermittelt worden sind, widerspricht dem Rechtsstaatsprinzip und ist grundsätzlich als nicht rechtmäßig anzusehen. Eine Verarbeitung oder Nutzung dieser Daten würde gegen § 13 LDSG verstoßen. Die Verwaltung darf ihrerseits nicht dazu beitragen, dass ihre Informanten gegen Rechtsvorschriften verstoßen. Das wäre aber jedenfalls dann der Fall, wenn sie aufgrund der Umstände von einem Rechtsverstoß des Informanten ausgehen muss und sie den Informanten zu solchen Rechtsverstößen ermutigen würde. Eine solche Konstellation hat hier nach Auffassung des LfD vorgelegen. Dies führt allerdings nicht zu einem

absoluten Verwertungsverbot. Die vorstehend dargelegte Rechtslage lässt eine Ausnutzung des rechtswidrigen Handelns einer anderen Person aber nur dann zu, wenn eine Abwägung der in Rede stehenden Rechtsgüter (in Anlehnung an die in § 34 StGB genannten Kriterien) die beabsichtigte Datennutzung trotz der Widerrechtlichkeit der erfolgten Übermittlung als angemessen und verhältnismäßig erscheinen lässt. Danach gilt: Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden. Hier war zunächst schon die Aussagekraft der in Rede stehenden unter Verstoß gegen das Bankgeheimnis übermittelten Informationen für das Ziel der Ausländerbehörde fraglich, die Einhaltung der aufenthaltsrechtlichen Bestimmungen des Ausländergesetzes zu ermöglichen sowie ggf. strafrechtlich gegen die Verletzung des § 92 AuslG vorzugehen. Eine solche Konstellation hätte weiter zur Voraussetzung, dass die zu schützenden Rechtsgüter (hier: die Einhaltung der ausländergesetzlichen Voraussetzungen für eine Verlängerung der Aufenthaltserlaubnis, möglicherweise auch der staatliche Strafanspruch wegen eines Verstoßes gegen § 92 AuslG) deutlich gegenüber der Wahrung des Bankgeheimnisses des betroffenen Dritten überwiegen.

Auch das Vorliegen einer solchen deutlichen Vorrangstellung für die öffentlichen Interessen konnte der LfD im vorliegenden Zusammenhang nicht erkennen. Aus seiner Sicht war die Nutzung der rechtswidrig übermittelten Informationen im vorliegenden Fall also unzulässig.

Das Ausländeramt wurde auf die vorstehend geschilderte Rechtslage und die darauf beruhende Beurteilung des konkreten Vorgangs hingewiesen. Es hat erklärt, diese Überlegungen in künftigen Fällen zu berücksichtigen.

12.4.2 Einsatz eines inoffiziellen Dolmetscher

Eine chinesische Studentin wurde durch ein Ausländeramt gebeten – da sie zufällig anwesend war – als Übersetzerin tätig zu werden. Sie sollte eine in chinesischer Schrift abgefasste Erklärung über die Einkommensverhältnisse einer anderen Chinesin übersetzen. Auf die Eingabe der betroffenen Studentin hin, der die „Übersetzerin“ von ihrer Tätigkeit berichtet hatte, überprüfte der LfD die Angelegenheit. Die Frage, ob für die „Übersetzerin“ eine Pflicht zur Übernahme dieser Tätigkeit bestand, hat er ausgeklammert, da sie keinen Datenschutzbezug hat; anzumerken ist aber, dass eine solche Pflicht wohl aus keinem rechtlichen Grund ableitbar sein dürfte.

Zu beurteilen war, ob das Ausländeramt eine zufällig beim Ausländeramt anwesende sprachkundige Person mit einer Sachverständigentätigkeit beauftragen und mit den dafür erforderlichen Informationen versehen durfte. Für die Beurteilung dieser Frage sind das Aufenthaltsgesetz und ergänzend das Verwaltungsverfahrensgesetz zugrunde zu legen. Nach § 23 VwVfG gilt, dass dann, wenn bei einer Behörde in einer fremden Sprache Dokumente vorgelegt werden, die Behörde unverzüglich die Vorlage einer Übersetzung verlangen soll. In begründeten Fällen kann die Vorlage einer beglaubigten oder von einem öffentlich bestellten oder beeidigten Dolmetscher oder Übersetzer angefertigten Übersetzung verlangt werden. Wird die Übersetzung nicht unverzüglich vorgelegt, so kann die Behörde auf Kosten des Beteiligten selbst eine Übersetzung beschaffen. Vor diesem Hintergrund hatte das Ausländeramt also grundsätzlich die Pflicht, für die Vorlage einer Übersetzung zu sorgen. Das Ausländeramt hatte hier im Interesse der Beschleunigung und nicht zuletzt, um der Betroffenen Kosten zu ersparen, den gerügten inoffiziellen und einfachen Weg gewählt. In Ansehung der Regelung des § 10 VwVfG – wonach das Verwaltungsverfahren an bestimmte Formen nicht gebunden ist, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen, und wonach es einfach, zweckmäßig und zügig durchzuführen ist – war diese Überlegung aus der Sicht des LfD zwar nachvollziehbar. Nach § 23 Abs. 2 VwVfG bedarf die Heranziehung eines öffentlich bestellten und vereidigten Übersetzers zudem eines besonderen Grundes.

Aus der Sicht des Datenschutzes kommt der Verpflichtung eines Sachverständigen zur Verschwiegenheit besondere Bedeutung zu. Diese Pflicht ist bei einem amtlich bestellten und vereidigten Sachverständigen sicherlich deutlicher und effizienter durchsetzbar als bei einem in Dienst genommenen Privaten. Allerdings ist auch der Private nicht völlig frei und ungebunden, was die Verwertung der erlangten Kenntnisse anbelangt. Er darf diese nicht unter Verstoß gegen die Persönlichkeitsrechte nutzen, ansonsten würde er sich gem. §§ 826, 823 Abs. 2 BGB schadensersatzpflichtig machen. In jedem Fall ist aber eine in Dienst genommene Privatperson auf die Rechtslage hinzuweisen, um vorbeugend im Sinne des Datenschutzes zu wirken. Nach Auffassung des LfD ist allerdings auch bei Einhaltung dieser Vorgaben eine andere Verfahrensweise als die vorliegend vom Ausländeramt gewählte vorzuziehen. Danach sollte eine ausländische Antragstellerin zunächst auf ihre Pflicht zur Vorlage einer eigenen Übersetzung hingewiesen werden. Bei Zweifeln an deren Richtigkeit könnte das Ausländeramt dann einen bestellten und vereidigten Übersetzer heranziehen.

Das betroffene Ausländeramt wurde auf diese Rechtsauffassung hingewiesen. Es erklärte, künftig entsprechend zu verfahren.

13. Finanzverwaltung

13.1 Weitere Entwicklung beim Kontendatenabruf

In seinem 20. Tb. unter Tz. 13.1 hatte der LfD nähere Ausführungen zu den Voraussetzungen für die aufgrund des „Gesetzes zur Förderung der Steuerehrlichkeit“ ab dem 1.4.2005 geschaffene Möglichkeit des Abrufs von Kontendaten von Bankkunden durch Finanzbehörden und andere öffentlichen Stellen gemäß § 93 Abs. 7 und Abs. 8 AO gemacht. Nach diesem Gesetz können Finanzbehörden und andere öffentliche Stellen über das BZSt bei den Kreditinstituten unter bestimmten Voraussetzungen Informationen über die Kontenstammdaten von Bankkunden erhalten.

Die Datenschutzbeauftragten des Bundes und der Länder hatten von Anfang an auf die fehlende Normenklarheit von § 93 Abs. 8 AO – welche Behörden außerhalb der Finanzverwaltung sind tatsächlich abrufberechtigt – und die unzureichende Information der Betroffenen über den Abruf hingewiesen. Den u.a. damit begründeten Antrag auf Erlass einer einstweiligen Anordnung gegen das Inkrafttreten der oben genannten Vorschriften hatte das Bundesverfassungsgericht abgelehnt, weil das BMF in einem Anwendungserlass zu den umstrittenen Regelungen die näheren Voraussetzungen für deren Umsetzung festgelegt hatte. Ausdrücklich betont hatte das Bundesverfassungsgericht aber, dass der Ausgang des Hauptsacheverfahrens offen sei.

Inzwischen hat das Bundesverfassungsgericht mit Beschluss vom 13.6.2007 entschieden, dass § 93 Abs. 8 AO – mit den von den Datenschutzbeauftragten nach wie vor vertretenen Argumenten – insofern an einem Bestimmtheitsmangel leide, als die Norm den Kreis der zugriffsberechtigten Behörden nicht hinreichend präzise festlege und daher Zugriffe für eine unübersehbare Vielzahl von Gesetzeszwecken ermögliche. Im Übrigen sei § 93 Abs. 8 AO ebenso wie § 93 Abs. 7 AO verfassungsrechtlich nicht zu beanstanden.

Durch das Unternehmensteuerreformgesetz 2008 wurde § 93 Abs. 8 AO mit Wirkung vom 18.8.2007 geändert und die Gesetzeszwecke, für die Zugriffe auf Kontendaten zulässig sind, konkret genannt. Gerichte sind nunmehr nicht mehr abrufberechtigt. Weiterhin wurden die Unterrichtung des betroffenen Steuerpflichtigen und die Dokumentationspflicht in den Absätzen 9 und 10 geregelt. Dies ist aus datenschutzrechtlicher Sicht zu begrüßen.

Nach Inkrafttreten der gesetzlichen Regelung für den Kontendatenabruf im Jahr 2005 haben die Landesdatenschutzbeauftragten die Durchführung der Abrufe bei den Finanzbehörden geprüft. Die dabei teilweise festgestellten Mängel bei der Dokumentation der Gründe für eine Ermessensentscheidung zur Vornahme eines Kontendatenabrufs durch den Sachbearbeiter haben die Datenschutzbeauftragten des Bundes und der Länder zum Anlass für die Bildung einer Projektgruppe genommen. Diese Projektgruppe hat einen Vorschlag für das formularmäßige Ersuchen eines Kontendatenabrufes nach § 93 Abs. 7 AO entwickelt. Der BfDI hat den Formularvorschlag dem BMF im September 2006 mit der Bitte übersandt, auf eine bundeseinheitliche Verwendung hinzuwirken. Der Vordruck wurde von den Bundesländern teilweise übernommen bzw. vorhandene Vordrucke entsprechend überarbeitet.

13.2 eTIN – electronic Taxpayer Identification Number

Gemäß § 41b Abs. 2 EStG hat der Arbeitgeber für die Datenfernübertragung der Lohnsteuerdaten aus dem Namen, Vornamen und Geburtsdatum des Arbeitnehmers ein Ordnungsmerkmal nach amtlich festgelegter Regel für den Arbeitnehmer zu bilden und zu verwenden. Das lohnsteuerliche Ordnungsmerkmal darf nur für die Zuordnung der elektronischen Lohnsteuerbescheinigung oder sonstiger für das Besteuerungsverfahren erforderlichen Daten zu einem bestimmten Steuerpflichtigen und für Zwecke des Besteuerungsverfahrens erhoben, gebildet, verarbeitet oder genutzt werden. Diese eTIN ist ein 14-stelliger Ordnungsbegriff, der aus den o. g. persönlichen Daten gebildet wird.

Haben verschiedene Personen den gleichen Namen und das gleiche Geburtsdatum, erhalten sie dieselbe eTIN und es kann zu Personenverwechslungen im Steuerverfahren kommen. Diese Gefahr besteht bei ca. 2 % aller Steuerpflichtigen. Dies kann zur Folge haben, dass dem einen Steuerpflichtigen Daten des anderen Steuerpflichtigen übermittelt werden und dadurch das Steuergeheimnis verletzt würde. Mehrere solcher Fälle wurden dem LfD bekannt. Das Finanzministerium verwies darauf, dass es sich bei der eTIN um eine Übergangslösung handele. Mit der Einführung der Steueridentifikationsnummer (s. Tz. 13.3) würden solche Personenverwechslungen ausgeschlossen werden. Für das Veranlagungsjahr 2007 wird es aber noch größtenteils zum Einsatz der eTIN und nicht der Steueridentifikationsnummer kommen. Daher hat der LfD nachdrücklich darauf hingewiesen, dass vor einer Bearbeitung von Steuererklärungen zunächst eine eindeutige Identifikation des Steuerpflichtigen erforderlich ist. In diesem Sinne sind die Mitarbeiter in den Finanzämtern zu sensibilisieren. Das Finanzministerium teilt diese Auffassung.

13.3 Einführung der Steueridentifikationsnummer zum 1.7.2007

Die für die Einführung der Steueridentifikationsnummer einschlägigen §§ 139a-d wurden mit dem Steueränderungsgesetz 2003 in die Abgabenordnung aufgenommen. Die auf § 139d AO als Verordnungsermächtigung beruhende StIdV ist am 7.12.2006 in Kraft getreten. Bislang wurde die Steuernummer nicht dauerhaft vergeben, sondern jedem Steuerzahler bei Umzügen neu erteilt. Ab 1.7.2007 bekommt nunmehr jede natürliche Person, auch Neugeborene (§ 1 EStG), eine lebenslange Steueridentifikationsnummer. Der Gesetzgeber möchte mit dieser Maßnahme eine Vereinfachung und Erhöhung der Transparenz des Besteuerungsverfahrens erreichen; letztendlich führt dies zu einer besseren Kontrolle der Steuerpflichtigen und soll u.a. der Eindämmung des Umsatzsteuerbetruges dienen. Aufgrund von Datenübermittlungen der Meldebehörden der Länder an das BZSt vergibt dieses eine Identifikationsnummer und speichert diese Daten (Familienname, frühere Namen, Vornamen, Doktorgrad, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, Geschlecht und gegenwärtige Anschrift). An der Erprobung des Verfahrens der Datenübermittlung von den Meldebehörden an das BZSt hat Rheinland-Pfalz mitgewirkt. Durch die Datenübermittlungen von den Meldebehörden an das BZSt wird eines von drei geplanten bundesweiten, vom Bund zu unterhaltenden zentralen Registern entstehen: Neben dem Register der Steueridentifikationsnummer ggf. noch das zentrale Melderegister beim Bundesverwaltungsamt und der Datenbestand für die Volkszählung beim Statistischen Bundesamt (s. Tz. 16.1).

Der BfDI hat im Laufe des Gesetzgebungsverfahrens einige Verbesserungen erreicht, z.B. die Reduzierung des Datenkatalogs der Datenbank beim BZSt, eine strikte Zweckbegrenzung auf steuerliche Zwecke (eine zweckwidrige Verwendung der Identifikationsnummer ist mit bis zu 10.000 Euro bußgeldbewehrt). Der BfDI konnte die Einführung der Identifikationsnummer aber nicht verhindern. Die Datenschutzbeauftragten des Bundes und der Länder haben daraufhin auf die Gefahr hingewiesen, dass sich aus der Einführung von einheitlichen Personennummern in verschiedenen Verwaltungsbereichen ein verfassungswidriges Personenkennzeichen entwickeln kann. Unter Bezugnahme auf das Volkszählungsurteil hat die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26.03.2004 im Rahmen einer Entschließung an den Gesetzgeber appelliert, solche Personennummern nur zuzulassen, wenn sie unerlässlich sind und der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsieht.

Auch im Laufe der Beratungen des Verordnungsentwurfs konnte der BfDI noch verschiedene datenschutzrechtliche Forderungen, wie Löschungs- und Informationsregelungen durchsetzen. Trotzdem bleiben die Zweifel des BfDI an dem Vorhaben bestehen, da nicht zu erkennen sei, dass effektive Besteuerungsverfahren und die Bekämpfung der Steuerhinterziehung zukünftig nur mittels lückenloser Registrierung aller Bürger von Geburt an möglich sein solle. Auch bestehe die Gefahr, dass die erreichte Zweckbindung später durch Gesetzesänderungen aufgeweicht und die beim BZSt entstehende Datenbank für andere Zwecke genutzt werde. Sobald Anzeichen ersichtlich werden, die auf entsprechende Begehrlichkeiten hindeuten, werden die Datenschutzbeauftragten dieser Gefahr entschieden entgegentreten.

13.4 Datenschutzgerechte Service-Center in den Finanzämtern

Die Einrichtung der Service-Center aller Finanzämter wird grundsätzlich nach einem landeseinheitlichen Konzept umgesetzt. Hierbei werden für die Abwicklung des Publikumsverkehrs offen gestaltete Beratungsboxen eingesetzt. Gerade diese Beratungsboxen gaben aber Anlass für mehrere Beschwerden seitens der Steuerpflichtigen. Diese Boxen seien so gestaltet, dass dort von Steuerpflichtigen Gespräche von Dritten mit dem Sachbearbeiter benachbarter Beratungsboxen mitgehört und diese auch gesehen werden können.

Auf die Eingaben hin fanden Ortsbesichtigungen durch Vertreter der OFD und Akustikfachleute des LBB statt. Teilweise wurden im Berichtszeitraum auch schon Schallschutzmaßnahmen getroffen. So wurden in einem Fall die Lochblecheinsätze der Beratungsboxen mit Dämmplatten verschlossen, um eine Schallreduzierung zu erzielen. Gleichzeitig dient dies auch dem Sichtschutz zwischen den einzelnen Boxen, um den Blickkontakt zwischen den Kunden bzw. den Sachbearbeitern unterschiedlicher Beratungsboxen nach Möglichkeit zu verhindern.

Die Service-Center sollen zwar grundsätzlich für die Abwicklung des gesamten Publikumsverkehrs zuständig sein. Dabei kommen als Serviceleistungen beispielsweise die Annahme von Voranmeldungen und Steuererklärungen, die abschließende Bearbeitung von Lohnsteuerermäßigungsanträgen und die Aufnahme von Niederschriften zu Anträgen und Einsprüchen in Betracht. Es ist aber zu berücksichtigen, dass mit der Inanspruchnahme der Angebote der Service-Center, die zur Erleichterung der Kundenkontakte mit den Finanzämtern eingerichtet wurden, ein gewisser Verzicht auf das Steuergeheimnis einhergeht. Doch es besteht immer die Möglichkeit, sich mit einem Mitarbeiter eines Service-Centers für ein Einzelgespräch in einen separaten Besprechungsraum zu begeben. Darüber hinaus ist es möglich, beispielsweise bei intensiver zu erörternden steuerlichen Problemen einen Termin mit dem zuständigen Sachbearbeiter zu vereinbaren, so dass man das Service-Center nicht aufsuchen muss.

Vor diesem Hintergrund besteht aus datenschutzrechtlicher Sicht kein Anlass, zur Wahrung des Steuergeheimnisses über die oben dargestellten Bemühungen und Maßnahmen der Finanzämter hinaus noch weitere bauliche Veränderungen zu fordern.

13.5 Bekanntgabe von Umsatzzahlen bei der Festlegung des Fremdenverkehrsbeitrages

Kein Unternehmen gibt gerne seine Umsatzzahlen preis. Der LfD hat sich im Rahmen der Festsetzung von Fremdenverkehrsbeiträgen immer wieder mit entsprechenden Sachverhalten zu beschäftigen. Im konkreten Fall ging es darum, ob aufgeschlüsselte Umsatzzahlen eines Hotelbetriebes dem Fremdenverkehrsausschuss einer Gemeinde vorgelegt werden durften.

Der Fremdenverkehrsausschuss hat gem. der Satzung über die Erhebung eines Fremdenverkehrsbeitrages die Aufgabe, Schätzungen vorzunehmen. Geschätzt wird u.a. der Umsatzanteil, der aus dem Fremdenverkehr erzielt wird. Fremdenverkehrsbeitragspflichtige Personen und Unternehmen legen der Gemeinde ihre Umsatzzahlen vor. Auf der Grundlage der vom Fremdenverkehrsausschuss vorgenommenen Schätzung wird der Fremdenverkehrsbeitrag aufgrund der konkreten Zahlen genau festgelegt. Gegen einen solchen Beitragsbescheid hatte ein ortsansässiger Hotelbetrieb Widerspruch eingelegt mit der Begründung, der geschätzte fremdenverkehrsbedingte Umsatzanteil sei zu hoch bemessen. Zur Begründung hatte der Hotelbetrieb eine Aufschlüsselung der einzelnen Umsätze für den Bereich Beherbergung und Gaststätte/Restaurant sowie Umsatz durch Gäste aus der Gemeinde und auswärtige Gäste vorgelegt. Bevor über den Widerspruch entschieden werden sollte, sollten diese Zahlen dem Fremdenverkehrsausschuss zur Überprüfung vorgelegt werden.

In der Regel erhält der Ausschuss keine genauen Umsatzzahlen einzelner Personen oder Unternehmen. Bei der Schätzung werden Art und Umfang der Tätigkeit, Lage und Größe der Geschäfts- und Beherbergungsräume, Betriebsweise, Zusammensetzung des Kundenkreises und die Zeitspanne berücksichtigt, in der die Tätigkeit innerhalb des Erhebungszeitraums ausgeübt wird. Umsatzzahlen werden danach nicht für die Schätzung herangezogen. Im vorliegenden Fall lag jedoch ein Widerspruch gegen die vorgenannte Schätzung und die darauf gestützte Festlegung des Fremdenverkehrsbeitrages vor. Da sich der Widerspruch auch gegen die vorausgegangene Schätzung richtete und der Widerspruchsführer mit der Vorlage von Umsatzzahlen sein Begehren begründete, hielt der LfD es im vorliegenden Fall für erforderlich, dass der Fremdenverkehrsausschuss für eine Überprüfung seiner Schätzung in diesem Einzelfall Umsatzzahlen erhielt. Aus dem Umsatzzahlen ließ sich z.B. ableiten, welche Summe ein einzelner Einwohner der Gemeinde in der Gaststätte pro Jahr ausgegeben haben muss, um den behaupteten Umsatzanteil zu erzielen. Dies war ein wesentlicher Gesichtspunkt für eine evtl. notwendige Berichtigung der Schätzung. Zudem sind die Mitglieder des Fremdenverkehrsausschusses zur Verschwiegenheit verpflichtet.

13.6 Informationsrechte kommunaler Gremien im Bauwesen

Mehrfach war durch den LfD zu beurteilen, welche Rechte kommunale Gremien hinsichtlich der Kenntnisnahme von in Baugenehmigungsverfahren erhobenen personenbezogenen Daten geltend machen können. Als Besonderheit zu beachten war dabei, dass die Gemeinden untere Bauaufsichtsbehörden sind. In einem Fall wurde der LfD um Prüfung gebeten, ob das Bauamt den Mitgliedern des Bau- und Umweltausschusses auf dessen entsprechenden Beschluss hin bezüglich aller Vorhaben im Gemeindegebiet Angaben zum Bauherrn, zur Baubeschreibung des jeweiligen Vorhabens sowie die genaue Lagebezeichnung und somit personenbezogene Daten übermitteln darf. Da dies ohne Einwilligung der Betroffenen erfolgen sollte, wäre dies nur zulässig gewesen, wenn eine Rechtsvorschrift dies erlaubt oder anordnet.

Dem Bau- und Umweltausschuss wurde gemäß § 32 Abs. 1 Satz 2 GemO i.V.m. § 3 Abs. 1 der Hauptsatzung u.a. die Entscheidung über die Erteilung des Einvernehmens der Gemeinde gemäß § 36 Abs. 1 Satz 1 BauGB übertragen. Hier kommt als Rechtsgrundlage für die Übermittlung personenbezogener Daten § 65 Abs. 5 Satz 2 LBauO (Behandlung des Bauantrags) i.V.m. § 14 Abs. 1 BauuntPrüfVO in Betracht, soweit diese für im Baugenehmigungsverfahren zu beteiligende Behörden für deren Entscheidung erforderlich sind. Allerdings ist § 36 Abs. 1 BauGB auf den Fall zugeschnitten, dass es sich bei der Baugenehmigungsbehörde nicht um eine Behörde der Gemeinde handelt. Ist die Gemeinde daher selbst zugleich Baugenehmigungsbehörde, so ist die Erteilung eines (förmlichen) Einvernehmens entbehrlich. In diesem Fall laufen dann die oben genannten Vorschriften für die Datenübermittlung ins Leere, da die Zulässigkeit der Datenübermittlung an eine von dem fraglichen Gremium zu treffende Entscheidung gebunden ist. Außerhalb von Baugenehmigungsverfahren kann auf die o.g. Rechtsgrundlage sowieso nicht zurückgegriffen werden.

Auch aus dem Unterrichtungs- und Kontrollrecht des Gemeinderats gemäß § 33 GemO konnte in diesem Zusammenhang keine Grundlage für die gewünschte Datenübermittlung abgeleitet werden. Denn diese Informationspflicht besteht nur gegenüber dem Gemeinderat in seiner Gesamtheit, nicht gegenüber einzelnen Ratsmitgliedern oder Fraktionen. Es besteht somit keine Berechtigung eines einzelnen Ausschusses als Teilorgan des Gemeinderates, Interessen wahrzunehmen, die nur dem Gemeinderat als Organ der Gemeinde in seiner Gesamtheit zustehen. Außerdem gelten § 33 Abs. 1 Satz 2, Abs. 3 und 4 GemO u.a. dann nicht, wenn überwiegende schutzwürdige Interessen Betroffener entgegenstehen (§ 33 Abs. 5 GemO.) Nach Ansicht des LfD steht das Recht auf informationelle Selbstbestimmung einer Datenübermittlung aufgrund von § 33 GemO immer dann entgegen, wenn ohne Bezug zu einem konkret zu entscheidenden Einzelfall gleichsam aus einem allgemeinen Informationsbedürfnis heraus um die Übermittlung personenbezogener Daten gebeten wird. Die von den Mitgliedern des Bau- und Umweltausschusses

gewünschte Übermittlung personenbezogener Daten hätte bei der gegebenen Sachlage nur aufgrund einer Einwilligung der Betroffenen erfolgen können.

In einem anderen Fall ging es um die Prüfung und Beantwortung der Frage, ob einer Ratsfraktion auf deren Antrag hin von der Verwaltung Informationen zum Antragsteller im Zusammenhang mit einem bestimmten Baugenehmigungsverfahren hätten übermittelt werden dürfen. Darüber hinaus wünschte die Ratsfraktion Auskünfte zu den gegen die Baugenehmigung eingelegten Nachbarwidersprüchen sowie zu dem in der Sache geführten Schriftwechsel mit der oberen Bauaufsichtsbehörde.

Auch in diesem Fall kamen weder bereichsspezifische Vorschriften des Bauordnungsrechts noch das oben bereits angesprochene Unterrichtungs- und Kontrollrecht zur Anwendung. § 65 Abs. 5 LBauO schied als Übermittlungsgrundlage aus, weil das Baugenehmigungsverfahren bereits abgeschlossen war. § 70 Abs. 4 LBauO und die darin geregelte Benachrichtigungspflicht der Verwaltung durch die Bauaufsichtsbehörde war nicht einschlägig, da die Gemeindeverwaltung selbst zugleich untere Bauaufsichtsbehörde ist. § 33 Abs. 3 GemO scheidet als Grundlage für die Nutzung personenbezogener Daten im Zusammenhang mit einem laufenden Widerspruchsverfahren bereits deshalb aus, weil der Stadtrechtsausschuss als Widerspruchsbehörde nicht den Weisungen der Organe der Gemeinde und somit auch nicht dem Kontrollrecht des Gemeinderats unterliegt. Ein Akteneinsichtsrechts des Gemeinderats gemäß § 33 Abs. 3 Satz 2 GemO bedarf eines berechtigten Interesses. Hinsichtlich der Subsumtion dieser Vorschrift konnte der LfD nur grundsätzliche Hinweise geben. Auch in einem solchen Fall dürfte ein berechtigtes Interesse regelmäßig nicht gegeben sein, wenn die Akteneinsicht ohne konkreten Anlass erfolgen und lediglich auf die allgemeine Kontrolle der Verwaltung abzielen würde.

14. Wirtschaft und Verkehr

14.1 Gewerbeanmeldungen über die IHK

Die IHK erhielt im Berichtszeitraum durch Landesverordnung die Befugnis, bestimmte Gewerbeanzeigen entgegen zu nehmen. Dadurch soll Existenzgründern, die sich z.B. durch die IHK beraten lassen, ein weiterer Weg zum Gewerbeamt erspart bleiben und der Weg in die Selbständigkeit weiter erleichtert werden. Die Kammer leitet die Gewerbeanzeigen an die zuständigen Behörden weiter und hat daher nur eine Briefträgerfunktion. Aus datenschutzrechtlicher Sicht war gegen diese Beauftragung der IHK nichts einzuwenden, zumal die Anmeldungen auch weiterhin bei den Gewerbeämtern vorgenommen werden können.

14.2 Webcams an der Autobahn

Einem Bürger fielen an der Autobahn Kameras auf. Er wollte vom LfD wissen, wie dies datenschutzrechtlich zu bewerten sei (s. a. Tz. 18.1).

Der Landesbetrieb Mobilität betreibt an einigen Straßen in Rheinland-Pfalz Webcams. Eine Liste der Webcams und die übertragenen Bilder sind im Internet abrufbar. Es erfolgt keine dauerhafte Übertragung der beobachteten Straßenabschnitte, sondern es werden lediglich Standbilder übertragen, die ca. jede Minute aktualisiert werden. Bei den vom LfD überprüften Bildern konnte nicht festgestellt werden, dass ein Kraftfahrzeugkennzeichen lesbar übertragen wurde. Somit handelt es sich nicht um die Aufzeichnung und Übertragung von personenbezogenen Daten. Damit war auch die weitere Zuständigkeit des LfD zur Überprüfung nicht gegeben. Der Landesbetrieb Mobilität stellt die Bilder zur Verfügung, um dem Straßennutzer eine Übersicht über die aktuelle Verkehrslage zu geben. Dies ist mit seiner Aufgabe, die Bundesautobahnen sowie die Bundes-, Landes- und Kreisstraßen in Rheinland-Pfalz zu betreuen, vereinbar.

15. Landwirtschaft, Weinbau und Forsten *(unbesetzt)*

16. Statistik

16.1 Volkszählung 2011 als registergestützter Zensus

Die EU wird für das Jahr 2011 gemeinschaftsweit Volks- und Wohnungszählungen vorschreiben. Das Bundeskabinett hat 2006 beschlossen, dass sich Deutschland mit einem registergestützten Verfahren an der Volkszählung beteiligen wird. Im September 2007 hat der Bundestag bereits das Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung (Zensusvorbereitungsgesetz 2011) verabschiedet.

Wichtigstes Ziel einer Volkszählung ist die Ermittlung amtlicher Einwohnerzahlen, die in vielerlei Hinsicht als maßgebliche Bemessungsgrundlagen dienen. Die Notwendigkeit für eine erneute Volkszählung wird laut der Gesetzesbegründung u.a. darin gesehen, dass die fortgeschriebenen Volkszählungszahlen und die darauf aufbauenden Statistiken mit zunehmendem Abstand zu den letzten Zählungen immer ungenauer wurden. So liegt z.B. die amtliche Bevölkerungszahl aus der Fortschreibung nach Schätzungen des Statistischen Bundesamtes um etwa 1,3 Millionen Menschen über der vermuteten Bevölkerungszahl in Deutschland.

Die Datenschutzbeauftragten des Bundes und der Länder haben das Gesetzgebungsverfahren begleitet und Anregungen geäußert. Daraufhin wurde hinsichtlich der Speicherdauer für das Anschriften- und Gebäuderegister festgelegt, dass dieses zum frühest möglichen Zeitpunkt nach Abschluss des Zensus, spätestens jedoch sechs Jahre nach dem Zensusstichtag gelöscht werden soll. Diese klare Regelung ersetzt nunmehr eine frühere weichere Formulierung.

Der entscheidende Unterschied zur 1987 durchgeführten Volkszählung besteht darin, dass nicht alle Einwohner befragt werden, sondern die Volkszählung im Wesentlichen über die Auswertung verschiedener Verwaltungsregister, z.B. des Melderegisters, durchgeführt wird. Die Bevölkerung wird dadurch von Auskunftspflichten entlastet. Im Rahmen einer ergänzenden Stichprobe sollen zur Sicherung der Datenqualität lediglich ca. sechs Millionen Personen befragt werden. Weiterhin ist beabsichtigt, ungefähr 17 Millionen Immobilieneigentümer mit einer postalischen Vollerhebung nach Angaben zu ihren Objekten zu befragen. Dafür muss aber als Kernaufgabe zunächst ein Anschriften- und Gebäuderegister aufgebaut werden, das beim Statistisches Bundesamt errichtet und betrieben werden soll.

Der BfDI hat gegen diese Grundkonzeption der Volkszählung in seinem 21. Tb. (2005-2006, Tz. 7.5) keine datenschutzrechtlichen Bedenken geäußert und erwartet auch keine vergleichbaren Diskussionen wie im Vorfeld der 1983 geplanten Volkszählung. In der Vorbereitung befindet sich derzeit der Entwurf eines Zensusausführungsgesetzes. Darin sollen Art und Umfang der zu erhebenden Merkmale sowie die Durchführungsmodalitäten des Zensus 2011 geregelt werden.

16.2 „Dauerbrenner“ Mikrozensus

Der Mikrozensus als jährliche repräsentative Befragung von einem Prozent der Bevölkerung führt immer wieder zu Fragen über das Verfahren. Für die ausgewählten Haushalte besteht im Kernbereich des Mikrozensus, also bei Fragen zur Bevölkerung, zum Arbeitsmarkt u.a., eine gesetzliche Auskunftspflicht. Um die Wahrnehmung dieser Pflicht zu erleichtern, besuchen Interviewer als Erhebungsbeauftragte des Statistischen Landesamtes nach vorheriger schriftlicher Ankündigung die Betroffenen, um die zu erhebenden Daten zu erfassen. Werden die ausgewählten Personen wiederholt nicht angetroffen, hinterlassen die Interviewer einen sog. Selbstausfüllerfragebogen. Falls Schwierigkeiten beim Ausfüllen des Fragebogens auftreten, können die Bürger auch die Unterstützung des Interviewers oder direkt des Statistischen Landesamtes in Anspruch nehmen. Zudem besteht die Möglichkeit, die Daten im Rahmen eines Telefoninterviews an das Statistische Landesamt zu übermitteln. Dagegen bestehen keine Einwände.

17. Personaldatenverarbeitung

17.1 Automatisierte Beihilfedatenverarbeitung

Bereits im 14. Tb. (Tz. 17.4.2) hatte der LfD seine grundsätzlichen Bedenken gegen eine weitgehend automatisierte Beihilfedatenverarbeitung im Zusammenhang mit der Einführung von „BABSY“ deutlich gemacht. Dass das Verfahren „BABSY“ gleichwohl noch als datenschutzverträglich bewertet werden kann, liegt vor allem daran, dass eine nur sehr eingeschränkte Verarbeitung medizinischer Sachverhalte erfolgt und die eingereichten Belege an den Beihilfeberechtigten zurück übersandt und somit bei der ZBV nicht dauerhaft vorgehalten werden. Aus Kostengründen beabsichtigt das Finanzministerium nunmehr eine Erweiterung

der Automation in diesem Zusammenhang. Der LfD wurde angesichts der Sensitivität der verarbeiteten Daten und der Größe des betroffenen Personenkreises frühzeitig mit der Angelegenheit befasst, um die aus seiner Sicht erforderlichen rechtlichen und technisch-organisatorischen Anforderungen einbringen zu können. Das beabsichtigte Einscannen der Belege und die damit verbundene automatisierte Datenverarbeitung hochsensibler medizinischer Fakten ist angesichts bestehender Auswertungs- und Zugriffsmöglichkeiten mit erheblichen Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden. Das Entstehen einer landesweiten Datei, die etwa nach Diagnosen (z.B. AIDS, Krebs), Medikamenten (z.B. Viagra) oder Behandlungsmethoden (z.B. Psychotherapie) personenbezogen ausgewertet werden könnte, wäre aus datenschutzrechtlicher Sicht nicht akzeptabel. Bereits die Einrichtung der sogenannten Beihilfeinformationsstelle (BIS) hatte nämlich zu einer datenschutzrechtlich bedenklichen Erweiterung der Zugriffsbefugnisse geführt.

Um sich einen Überblick über die derzeitige automatisierte Verarbeitung von Beihilfedaten zu verschaffen, traf der LfD zum Verfahren „BABSY" örtliche Feststellungen bei der ZBV in Koblenz. Ziel der Kontrolle war es festzustellen, inwieweit bereits jetzt in „BABSY“ eine Verarbeitung medizinischer Sachverhalte erfolgt, um aus datenschutzrechtlicher Sicht beurteilen zu können, in welchem Umfang durch das beabsichtigte Einscannen hier Veränderungen zu erwarten sind.

Im Einzelnen hat die Prüfung der Software „BABSY“ Folgendes ergeben:

Von den Belegen werden derzeit lediglich Rechnungsdatum und -betrag manuell in die EDV übertragen. Eine Speicherung der Diagnose oder der sonstigen sich auf der Arztrechnung befindlichen medizinischen Sachverhalte erfolgt nicht. Medizinische Daten werden in „BABSY“ – so wie bei der Einführung 1992 mit dem LfD abgestimmt – nur eingeschränkt verarbeitet.

Eine Änderung gegenüber den Anmeldeunterlagen ist lediglich insoweit erfolgt, als nunmehr auch Bezügedaten durch die ZBV zur Berechnung der Kostendämpfungspauschale bzw. für Pflegeleistungen geliefert werden.

Allerdings werden eigene Beihilfeanträge von Mitarbeitern der ZBV derzeit nicht gesondert behandelt, die Bearbeitung erfolgt – mit Einverständnis der Personalvertretung – gegenseitig. Eine vergleichbare Situation besteht bei Beschäftigten einer Krankenversicherung. Hierzu regelt § 35 Abs. 1 Satz 3 SGB I, dass Sozialdaten der Beschäftigten und ihrer Angehörigen von Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein dürfen noch von Zugriffsberechtigten weitergegeben werden dürfen. Der LfD regte daher an, dies innerhalb der ZBV entsprechend zu praktizieren.

Was die Erweiterung der automatisierten Beihilfedatenverarbeitung angeht, wies der LfD auf folgende rechtliche Gesichtspunkte hin:

Durch das beabsichtigte Einscannen der Belege werden künftig – auch nach Einschätzung der ZBV – mehr Daten erfasst und gespeichert, als dies für die Beihilfeabrechnung tatsächlich erforderlich ist. Betroffen sind insbesondere Diagnose- und Behandlungsdaten. Darüber hinaus sieht die derzeitige Rechtslage ausdrücklich vor, dass die Belege an die Betroffenen unverzüglich zurückzusenden sind (§ 102 f Abs. 2 LBG). Sofern das Rücksenden der Belege künftig entfallen soll, müsste daher eine entsprechende Änderung des Landesbeamtengesetzes (und der VV) erfolgen.

Vor dem Hintergrund, dass die ZBV den Markt hinsichtlich in Betracht kommender EDV-Lösungen für die automatisierte Belegverarbeitung sondierte, wurden ihr folgende Punkte mitgeteilt, die in technischer Hinsicht für eine datenschutzgerechte Gestaltung von Bedeutung sind und daher bei der Auswahl des Verfahrens berücksichtigt werden sollten:

In den Bilddateien der eingescannten Beihilfeunterlagen sind zunächst die gesamten Informationen der Papierbelege enthalten. Diese Informationen können durch optische Zeichenerkennung in weiterverarbeitbare elektronische Daten überführt werden. Aus datenschutzrechtlicher Sicht ist daher darauf hinzuwirken, dass lediglich die für die Bearbeitung des Beihilfeantrages erforderlichen Daten in das Verfahren BABSY übernommen und weitergehende Informationen umgehend gelöscht werden. Die für die Beihilfebearbeitung erforderlichen Angaben aus den Belegen sind dabei im Einzelnen festzulegen. Zur Sicherung der Bilddateien sollten diese verschlüsselt gespeichert und elektronisch signiert werden, damit eine unbefugte Kenntnisnahme oder Veränderung der Informationen ausgeschlossen ist. Dies ist insbesondere dann erforderlich, wenn die Originalbelege nach der optischen Erfassung vernichtet werden und ggf. aus den elektronischen Daten Papierbelege rechtssicher wiederhergestellt werden sollen.

Für die eingescannten Belege sind Speicherfristen festzulegen, nach deren Ablauf die Belege zu löschen sind. Das Verfahren sollte es ermöglichen, dass die Löschung nicht mehr benötigter Belege automatisiert erfolgt. Nicht mehr benötigte Belegdaten sind nach Ablauf der entsprechend festzulegenden Zeiträume ebenfalls zu löschen bzw. im Falle einer weiteren Speicherung für statistische Auswertungen zu anonymisieren.

Soweit die in elektronischer Form vorgehaltenen Belege nicht in das Berechtigungskonzept des Verfahrens BABSY eingebunden sind, ist eine separate Rechteverwaltung vorzusehen, die sicherstellt, dass Zugriffe nur entsprechend der aufgabenbezogenen

Zuständigkeit der Nutzer erfolgen können. Befugte Zugriffe sowie unbefugte Zugriffsversuche sind auch hier zu protokollieren. Die entsprechenden Protokolldaten sind regelmäßig auszuwerten und auf etwaige Auffälligkeiten in der Nutzung zu prüfen (§ 9 Abs. 2 Ziff. 10 LDSG).

Auskunftsansprüchen der Betroffenen nach § 18 Abs. 3 LDSG sollte aus dem Verfahren heraus entsprochen werden können. In den Fällen des § 19 Abs. 3 LDSG muss das Verfahren die Sperrung einzelner Belege ermöglichen.

Um dem Problem der Erfassung nicht erforderlicher medizinischer Daten begegnen zu können, empfahl der LfD, bereits bei der Auswahl einer geeigneten Software darauf zu achten, dass diese über entsprechende Unterdrückungsfunktionen verfügt. Sollte dies nicht möglich sein, müssen Auswertungen in Bezug auf die erfassten medizinischen Daten systemtechnisch ausgeschlossen sein.

Von seiten des LfD wird auch weiterhin eine kritische Begleitung des Projekts erfolgen.

17.2 Die Kontrolle der Kontrolleure

Ein Hilfspolizist beschwerte sich beim LfD darüber, dass die bei der Überwachung des ruhenden Verkehrs zum Einsatz kommenden mobilen Datenerfassungsgeräte für Zwecke einer Verhaltens- und Leistungskontrolle durch die Stadtverwaltung „missbraucht“ würden. Die Arbeitsweise sehe so aus, dass nach Dienstende die erfassten Daten der „Verkehrssünder“ in die EDV des Amtes übertragen würden. Da das Gerät auch die Zeitpunkte der Verwarnungen speichere, müssten sich die Hilfspolizisten immer öfter rechtfertigen, was sie zwischen den einzelnen Verwarnungen gemacht hätten und über Anzahl und Höhe der Verwarnungen Rechenschaft ablegen.

Datenschutzrechtlich liegt in der mitarbeiterbezogenen Auswertung der erfassten Daten eine zweckändernde Datennutzung. Diese ist gem. § 13 Abs. 2 (i.V.m. § 12 Abs. 4 Ziff. 1) LDSG dann zulässig, wenn eine Rechtsvorschrift dies vorsieht. Im vorliegenden Fall konnte allenfalls eine Dienstvereinbarung als Rechtsvorschrift in diesem Sinne herangezogen werden. Diese lag jedoch nicht vor. Der LfD nahm unter Hinweis auf die Mitbestimmungstatbestände des § 80 Abs. 2 Ziff. 2 und Ziff. 3 LPersVG Kontakt mit dem behördlichen Datenschutzbeauftragten der Stadtverwaltung auf. Dieser sorgte dafür, dass in einem gemeinsamen Gespräch mit allen Beteiligten bestehende Missverständnisse ausgeräumt werden konnten und der Abschluss einer Dienstvereinbarung auf den Weg gebracht wurde. Das Beispiel zeigt, wie wichtig es ist, vor Ort eine Datenschutzfachkraft zu haben, die in Kenntnis der Besonderheiten der Dienststelle imstande ist, auch ohne weitere Beteiligung des LfD datenschutzverträgliche Lösungen zu finden.

17.3 Orientierungshilfe „Datenschutz und Zeiterfassung“

Aufgrund vermehrter Anfragen und der fortschreitenden Automation im Bereich der Personaldatenverarbeitung sah sich der LfD veranlasst, folgende Hinweise zum Datenschutz bei der elektronischen Zeiterfassung zu geben, die insb. beim Abschluss einer Dienstvereinbarung zwischen Dienststelle und Personalvertretung hilfreich sein können:

- Die Arbeitszeitverordnung regelt in § 12 Abs. 7, dass die erfassten Arbeitszeitdaten nur für die Überprüfung der Einhaltung der Arbeitszeit sowie für besoldungsrechtliche Zwecke verwendet werden dürfen und spätestens nach zwei Jahren zu löschen sind. Soweit tarifvertraglich nichts anderes bestimmt ist, ist diese für den Bereich der Beamten geltende Regelung für die sonstigen Beschäftigten des öffentlichen Dienstes entsprechend anzuwenden.
- Ob Zeiterfassungsdaten als Personalaktendaten im Sinne des § 102 Abs. 1 Satz 2 LBG zu qualifizieren sind und damit unter den besonderen Schutz des Personalaktengeheimnisses fallen, wird unterschiedlich beurteilt. Jedenfalls handelt es sich um personenbezogene Sachaktendaten, deren Verarbeitung nach allgemeinen Datenschutzgrundsätzen erforderlich und verhältnismäßig sein muss.
- Die Arbeitszeitverordnung selbst schützt mit ihrer engen Zweckbestimmung nur die Einzelbuchungen; Auswertungen in Form einer aktuellen Ab- bzw. Anwesenheitsliste, Krankheits- oder Urlaubsliste werden hierdurch nicht ausgeschlossen.
- Soll eine Anwesenheitsliste der Mitarbeiter für Auskünfte gegenüber anfragenden Bürgern online oder in Papierform zur Verfügung gestellt werden (z.B. Bürgerbüro, Telefonzentrale, Pforte), darf der Abwesenheitsgrund nicht mitgeteilt werden. Keine Bedenken bestehen dagegen, die voraussichtliche Rückkehr des Mitarbeiters anzugeben.
- Sofern Vorgesetzte über eine entsprechende Personalverantwortung verfügen, dürfen sie zu Kontrollzwecken im erforderlichen Umfang Kenntnis von den Zeiterfassungsdaten erhalten. Der LfD vertritt dabei die Auffassung, dass es grundsätzlich ausreichend ist, Vorgesetzten eine Monatsübersicht mit den geleisteten Ist/Soll-Stunden zur Verfügung zu stellen und sie darüber hinaus anlassbezogen (beispielsweise auffällige Über- oder Unterschreitung des Solls) zu unterrichten. Auch gegen Stichprobenkontrollen durch Vorgesetzte ist datenschutzrechtlich nichts einzuwenden. Ein Onlinezugriff auf die Einzelbuchungen der Mitarbeiter durch Vorgesetze ist dabei weder erforderlich noch verhältnismäßig; er ist nur dann

datenschutzrechtlich hinnehmbar, wenn eine entsprechende Regelung in der Dienstvereinbarung eine derart weitgehende Kontrolle ausdrücklich vorsieht.
- Auf der Basis von Zeiterfassungsdaten erstellte Urlaubs- oder Krankheitslisten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft vorgehalten und genutzt werden. Sie sind vor unbefugter Kenntnisnahme zu schützen und unverzüglich zu löschen, wenn sie nicht mehr benötigt werden.
- Der Personalvertretung dürfen die Zeiterfassungsdaten nur in anonymisierter oder pseudonymisierter Form zur Verfügung gestellt werden.
- Aus Gründen der Transparenz und zur Selbstkontrolle sollte den Beschäftigten der Zugriff auf ihr eigenes Zeitkonto eröffnet werden.

17.4 Datenschutz als Schutz des Betroffenen vor sich selbst?

Nach einer amtsärztlichen Untersuchung bat der Beamte einer Hochschule um Übersendung des Gutachtens. Die Personalstelle lehnte dies jedoch mit dem Hinweis ab, die Verwaltungsvorschrift zum Personalaktenrecht sehe dies nicht vor. Auch gebiete „ein sensibler Umgang mit den vertraulichen Unterlagen“ diese Vorgehensweise. Der Betroffene wies in seiner Eingabe an den LfD darauf hin, dass es nicht Zweck des Datenschutzes sein könne, seine eigenen Daten vor ihm als Betroffenen zu schützen.

Der LfD machte im Rahmen seiner datenschutzrechtlichen Würdigung gegenüber der Hochschule deutlich, dass § 102c LBG vorliegend als Rechtsgrundlage heranzuziehen ist. Nach dieser Vorschrift hat der Beamte das Recht auf Einsicht in seine vollständige Personalakte. Die Vorschrift besagt weiterhin, dass Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden können, soweit dienstliche Gründe nicht entgegenstehen. Nach Auffassung des LfD gebietet auch nicht „ein sensibler Umgang mit den vertraulichen Unterlagen“ die praktizierte Vorgehensweise: Es ist sicher richtig, dass bei einer Versendung des Gutachtens auf dem Postweg die Möglichkeit der Kenntnisnahme durch unbefugte Dritte besteht. Wenn der Betroffene jedoch, so wie hier, die Versendung ausdrücklich wünscht, bestehen keine Bedenken, wenn diesem Wunsch ggf. nach einem allgemeinen Hinweis auf die Risiken bei der Versendung von Schriftstücken entsprochen wird. Andernfalls könnte – wie der vorliegende Fall zeigt – leicht der Eindruck entstehen, „der Datenschutz“ verhindere die Wahrnehmung von Betroffenenrechten. Es bedurfte erstaunlicherweise einiger Überzeugungsarbeit, bis die Hochschule schließlich einlenkte und zusagte, künftig entsprechend der Rechtsauffassung des LfD zu verfahren.

18. Datenschutz im kommunalen Bereich

18.1 Einsatz von Webcams durch Kommunalverwaltungen

Mit der datenschutzrechtlichen Bewertung des Einsatzes von Webcams durch rheinland-pfälzische Kommunen hatte sich der LfD im Berichtszeitraum wiederholt zu befassen. Gegenstand waren die zu touristischen Zwecken über das Internetangebot der einzelnen Kommunalverwaltungen zur Verfügung gestellten Bilder, die mit einer eigens hierfür installierten Videokamera (Webcam) aufgenommen worden waren. Eine Aktualisierung der mit einer Zeitangabe versehenen Aufnahmen erfolgte zumeist minütlich.

Während im Regelfall die Bilder lediglich allgemeine Impressionen aus der Gemeinde ohne jegliche Verbindung zu einer Person zum Gegenstand hatten, fanden sich vereinzelt allerdings auch Kameraeinstellungen, bei denen ein solcher Personenbezug entweder offensichtlich bestand oder zumindest nicht ausgeschlossen werden konnte. So richtete sich in einem Fall die Webcam auf einen städtischen Brunnen, dessen Betrachter ohne weiteren Aufwand erkannt werden konnten. In einem anderen Fall betrafen die Aufnahmen einen zentralen Platz mit unmittelbar anliegenden Büro- und Wohngebäuden. Auch wenn Personen oder Autokennzeichen hier nicht direkt erkennbar waren, bestand durchaus die Möglichkeit, dass mit einem geringen Zusatzwissen die betreffenden Büro- und Wohngebäude einzelnen Personen zugeordnet werden konnten. Es war zu befürchten, dass durch die minütlichen Aktualisierungen der im Internet verfügbaren Bilder ein Verhaltensprofil der von diesen Aufnahmen betroffenen Personen bzw. der ihnen zuordenbaren Objekte möglich wurde.

Der LfD hat gegenüber den betroffenen Kommunalverwaltungen folgende Rechtsauffassung vertreten:
- Der Einsatz von Webcams durch öffentliche Stellen des Landes ist datenschutzrechtlich unzulässig, sofern dabei personenbezogene Daten übermittelt werden. Es kann dahin gestellt bleiben, ob in diesem Zusammenhang die Norm des § 34 Abs. 1 LDSG die allgemeine datenschutzrechtliche Bestimmung zur Datenübermittlung an Stellen außerhalb der öffentlichen Verwaltung verdrängt, da die Voraussetzungen beider Regelungen nicht vorliegen.

- Maßgebliches Kriterium für die Frage der datenschutzrechtlichen Zulässigkeit eines derartigen Einsatzes ist daher das Vorliegen von personenbezogenen Aufnahmen. Dies ist auch dann schon gegeben, wenn die darin enthaltenen Informationen personenbeziehbar sind, d.h. wenn Personen identifiziert oder Sachen natürlichen Personen zugeordnet werden können.
- Bezogen auf den Einsatz von Webcams hat das zur Folge, dass ein derartiger Einsatz datenschutzrechtlich immer dann als unzulässig zu bewerten ist, wenn auf den Aufnahmen die Gesichter von Personen oder die Kennzeichen von Fahrzeugen eindeutig zu erkennen sind. In Zweifelsfällen, d.h. wenn das Vorliegen personenbeziehbarer Aufnahmen nicht völlig ausgeschlossen werden kann, ist ein Einsatz von Webcams datenschutzrechtlich nur hinnehmbar, wenn nicht mehr als vier im Laufe eines Tages zu unterschiedlichen Zeiten aufgenommene Bilder der Öffentlichkeit zur Verfügung gestellt werden.

Mit der Beschränkung der täglich zulässigen Zahl von Bildaktualisierungen in den o.g. Zweifelsfällen möchte der LfD unter Wahrung des Datenschutzes dem Wunsch vieler Kommunalverwaltungen nach einer modernen und aktuellen eigenen Darstellung im Internet Rechnung tragen. Sofern die Bildung von Verhaltensprofilen faktisch ausgeschlossen ist, erscheint dem LfD in derartigen Fällen der Einsatz von Webcams noch hinnehmbar. Die dargestellte Rechtsauffassung wurde mit den betroffenen kommunalen Spitzenverbänden abgestimmt. Zugleich wurde vereinbart, dass die Mitglieder über die in diesem Zusammenhang bestehenden datenschutzrechtlichen Vorgaben informiert werden. Nach der Recherche der Verbände setzen gegenwärtig ca. 15 Kommunalverwaltungen im Lande Webcams im Rahmen ihres Internetauftritts ein.

18.2 Videoüberwachung öffentlicher Räume durch die allgemeinen Ordnungsbehörden

Mit den sinkenden Kosten und der höheren Leistungsfähigkeit der mittlerweile verfügbaren Videoüberwachungssysteme nimmt auch die Zahl der Kommunalverwaltungen zu, die zur Erfüllung der den Ordnungsbehörden obliegenden Aufgaben eine Überwachung öffentlich zugänglicher Räume durch Videokameras erwägen. So haben den LfD im Berichtszeitraum verstärkt Anfragen von Kommunen erreicht, die derartige Maßnahmen zum Schutz vor drohenden Beeinträchtigungen wie z.B. Sachbeschädigungen, Lärmbelästigungen oder Verunreinigungen beabsichtigten. Die Maßnahmen zielten dabei in der Regel auf eine personengenaue Beobachtung und Bildaufzeichnung ab.

Unter Berücksichtigung der in diesem Zusammenhang seitens des ISM abgegebenen polizeirechtlichen Bewertung vertritt der LfD folgende Rechtsauffassung:

Nach § 27 Abs. 1 POG sind die allgemeinen Ordnungsbehörden und die Polizei zur Erhebung personenbezogener Daten in öffentlich zugänglichen Räumen durch den offenen Einsatz technischer Mittel zur Bildübertragung befugt, soweit dies im Einzelfall zur Erfüllung einer Aufgabe nach § 1 Abs. 1 Satz 1 und 3 und Abs. 2 und 5 POG erforderlich ist. Eine Bildaufzeichnung ist in öffentlich zugänglichen Räumen nur zulässig, soweit dies im Einzelfall zur Abwehr einer Gefahr, zum Schutz gefährdeter öffentlicher Anlagen und Einrichtungen, zur Abwehr von Gefahren durch den Straßenverkehr oder zur Wahrnehmung von durch andere Rechtsvorschriften übertragenen Aufgaben erforderlich ist.

Angesichts der Grundrechtsrelevanz einer derartigen Maßnahme kommt dabei der Beachtung des Verhältnismäßigkeitsgrundsatzes besondere Bedeutung zu. Dies hat zur Folge, dass aus datenschutzrechtlicher Sicht der in diesem Zusammenhang beabsichtigte Einsatz von Videokameras nur dann als zulässig erachtet werden kann, wenn es sich bei dem Ort, der überwacht werden soll, auf Grund der Vielzahl der Delikte um einen Kriminalitätsbrennpunkt handelt. Dies setzt voraus, dass sich die Kriminalitätsbelastung des Ortes deutlich von der an anderen Orten abheben muss, konkrete Anhaltspunkte die Annahme rechtfertigen, dass am fraglichen Ort in Zukunft weitere Straftaten begangen werden und die Videoüberwachung zu deren Bekämpfung erforderlich ist (vgl. hierzu Urteil des VGH Baden-Württemberg vom 21.07.2003, NVwZ 2004, S. 498 ff.).

Sofern im Einzelfall eine der Erfüllung ordnungsbehördlicher Aufgaben dienende Videoüberwachung den dargestellten Anforderungen des § 27 Abs. 1 POG nicht genügt, muss von dieser Abstand genommen werden. Ein Rückgriff auf die in § 34 LDSG enthaltene Bestimmung scheidet aus, da § 27 POG als speziellere Regelung die Bildbeobachtung und -aufzeichnung durch die allgemeinen Ordnungsbehörden abschließend regelt.

18.3 Direktzugriffe für Ortsbürgermeister auf das Ratsinformationssystem?

Sofern Ortsbürgermeistern ein uneingeschränkter Direktzugriff auf das Ratsinformationssystem der VG (Sitzungssoftware) eingerichtet werden soll, betrifft dies zwangsläufig auch personenbezogene Inhalte. Insbesondere dann, wenn es sich um personenbezogene Daten im Zusammenhang mit nichtöffentlichen Sitzungen des Verbandsgemeinderates handelt, ist dies aus der Sicht des Datenschutzes von besonderer Bedeutung.

Maßgebliche Rechtsgrundlage für die Beurteilung der datenschutzrechtlichen Zulässigkeit ist § 7 LDSG. Nach Absatz 1 ist ein derartiges Verfahren nur zulässig, wenn es unter Berücksichtigung der schutzwürdigen Belange der Betroffenen, des Schutzes besonderer Berufs- oder Amtsgeheimnisse und der Aufgaben der beteiligten öffentlichen Stellen angemessen ist. Hierbei sind zunächst die gesetzlich vorgesehenen Informationsmöglichkeiten der Ortsbürgermeister zu beachten. Hinsichtlich der Sitzungen des Verbandsgemeinderates steht den Ortsbürgermeistern nach § 69 Abs. 3 GemO zwar ein Teilnahmerecht zu; nach Auffassung des LfD beschränkt sich dieses jedoch zumindest dann, wenn nichtöffentliche Sitzungen betroffen sind, nur auf solche, in denen die Belange der Ortsgemeinde berührt werden. Unabhängig von der Reichweite dieses Teilnahmerechtes haben nach § 41 Abs. 2 GemO jedoch nur Ratsmitglieder ein Zugangsrecht zu Niederschriften nichtöffentlicher Gemeinderatssitzungen. Auf der anderen Seite sind die Ortsbürgermeister nach § 69 Abs. 4 Satz 3 GemO durch den Verbandsgemeindebürgermeister über alle wichtigen Angelegenheiten, welche die Belange der Ortsgemeinden berühren, rechtzeitig zu unterrichten. Die Einrichtung uneingeschränkter Direktzugriffsmöglichkeiten für Ortsbürgermeister auf das Ratsinformationssystem der VG begegnet daher datenschutzrechtlichen Bedenken. In den Fällen, in denen durch den Zugriff auch personenbezogene Daten aus nichtöffentlichen Sitzungen des Gemeinderates erfasst werden und die Belange der Ortsgemeinde nicht betroffen sind, fehlt es bereits an der Erforderlichkeit eines derartigen Datenzugriffs. Gegenüber einer anfragenden VG vertrat der LfD die dargestellte Rechtsauffassung. Die Kommunalverwaltung ermöglichte den Ortsbürgermeistern unter Beachtung dieser Vorgaben den Zugang zum Ratsinformationssystem.

18.4 Widerspenstiger Ortsbürgermeister

In einem nicht alltäglichen Fall erwies sich ein Ortsbürgermeister trotz formeller Beanstandung durch den LfD und Einschaltung der Kommunalaufsicht als besonders beratungsresistent. Der Angelegenheit lag ein Streit zwischen einem Bürger und einer Ortsgemeinde über Schäden an einem öffentlichen Drainagerohr zugrunde. Nachdem der Bürger gegenüber der Ortsgemeinde eine Schadensersatzforderung gerichtlich geltend gemacht hatte, wurden in einem Ortstermin Schäden an dem besagten Rohr festgestellt. Der Ortsbürgermeister unterrichtete den Ortsgemeinderat in einer öffentlichen Ratssitzung unter ausdrücklicher Bezugnahme auf den betroffenen Bürger über dessen Schadensersatzforderung und den in diesem Zusammenhang erfolgten Ortstermin. Die Sitzungsniederschrift wurde im amtlichen Teil des Gemeindeblatts der VG veröffentlicht; sie enthielt neben dem Hinweis auf den Bürger die Information, dass beim „Ortstermin am [...] keinerlei Schäden im Drainagerohr“ festgestellt wurden.

Nach Auffassung des LfD stellten sowohl die Behandlung der Angelegenheit im öffentlichen Teil der Ratssitzung als auch die diesbezügliche Veröffentlichung der Sitzungsniederschrift im Gemeindeblatt der Verbandsgemeinde einen Verstoß gegen datenschutzrechtliche Vorgaben dar:

Hinsichtlich der Erörterung der Sache in öffentlicher Sitzung ergab sich dies aus § 35 Abs. 1 GemO, wonach Sitzungen des Gemeinderats grundsätzlich öffentlich sind, sofern nicht ausdrücklich etwas anderes bestimmt oder die Beratung in nichtöffentlicher Sitzung der Natur des Beratungsgegenstandes nach erforderlich ist. Entsprechend der Mustergeschäftsordnung für Gemeinderäte in Rheinland-Pfalz legte die im konkreten Fall geltende Geschäftsordnung für den Ortsgemeinderat ausdrücklich fest, dass die Öffentlichkeit u.a. dann auszuschließen ist, wenn persönliche Angelegenheiten der Einwohner oder Rechtsstreitigkeiten, an denen die Ortsgemeinde beteiligt ist, betroffen sind. Dies war aber gerade in der zugrunde liegenden Angelegenheit der Fall. Soweit die Sitzungsniederschrift insoweit im Gemeindeblatt der Verbandsgemeinde veröffentlicht wurde, fehlte es zugleich an einer erforderlichen Rechtsgrundlage. Denn datenschutzrechtlich stellte diese von der Ortsgemeinde veranlasste Veröffentlichung eine Datenübermittlung i.S.v. § 3 Abs. 2 Nr. 4 LDSG dar, für deren Zulässigkeit es mangels einer Einwilligung des Betroffenen einer Rechtsgrundlage bedurft hätte. Diese lag jedoch nicht vor. Nach § 41 Abs. 5 GemO soll die Gemeindeverwaltung die Einwohner über die Ergebnisse der Ratssitzungen in geeigneter Form unterrichten. Nach Nr. 7.1 der VV zu § 41 GemO bezieht sich diese Verpflichtung jedoch gerade nicht auf die Sitzungsniederschrift, sondern lediglich auf den sachlichen Inhalt der für die Einwohner wichtigen Ratsbeschlüsse, so dass diese Regelung nicht herangezogen werden konnte. Auch § 41 Abs. 4 GemO stellt lediglich ein Einsichtsrecht der Einwohner in die Niederschrift öffentlicher Sitzungen dar und gerade keine Befugnis der Gemeindeverwaltung, diese zu veröffentlichen. Es konnte schließlich dahin gestellt bleiben, ob angesichts dieser kommunalrechtlichen Vorgaben überhaupt noch Raum für die Anwendung von § 16 LDSG bleibt, da auch dessen Voraussetzungen im konkreten Fall nicht vorlagen.

Trotz dieser datenschutzrechtlichen Bewertung hielt es der betroffene Ortsbürgermeister nicht für geboten, in der Angelegenheit mit dem LfD zu kooperieren. Im Gegenteil, er drohte sogar mit der Einschaltung eines Rechtsanwaltes, sollte der LfD ihm noch weitere Rückfragen stellen. Auch die darauf hin ausgesprochene formelle Beanstandung des festgestellten Datenschutzverstoßes sowie die Einschaltung der Kommunalaufsicht beeindruckten den Ortsbürgermeister zunächst wenig. Erst nach weiteren intensiven Bemühungen teilte die Kommunalaufsicht mit, dass der kommunale Würdenträger ihr gegenüber die künftige Einhaltung der datenschutzrechtlichen Vorgaben glaubhaft versichert habe.

18.5 Veröffentlichung von Angaben zu Lohnersatzleistungen für einen freigestellten Ortsbürgermeister in der Presse

Zu einer formellen Beanstandung führten die in einer Regionalzeitung von einem Verbandsgemeindebürgermeister gemachten Angaben zu den von der VGV für einen Ortsbürgermeister jährlich aufzubringenden Lohnersatzleistungen. In dem zugrunde liegenden Fall hatte der Verbandsgemeindebürgermeister neben der Höhe der Leistungen auch die Zahl der Freistellungstage im Jahr genannt, so dass das von dem Betroffenen bezogene Grundgehalt von jedermann ausgerechnet werden konnte. Dies stand im Widerspruch zu den gesetzlichen Regelungen des Landesbeamtengesetzes und war daher datenschutzrechtlich unzulässig.

Die den Ortsbürgermeister betreffenden Angaben über die jährlich von der VGV an seinen Arbeitgeber gewährten Lohnersatzleistungen stellen angesichts des nach § 51 Abs. 1 GemO bestehenden Ehrenamtes ein Personalaktendatum i.S.v. § 102 Abs. 1 Satz 2 LBG dar. Die datenschutzrechtliche Zulässigkeit der Verarbeitung derartiger Daten richtet sich – auch bei Ehrenbeamten – nach den §§ 102 ff. LBG. Hiernach ist eine Weitergabe von Personalaktendaten an Dritte grundsätzlich nur mit Einwilligung des Beamten zulässig, es sei denn, die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz höherrangiger Interessen des Dritten erfordern die Datenübermittlung. Dies war hier nicht der Fall, so dass mangels Einwilligung des Betroffenen die Presse über die Höhe des von der VGV geleisteten Lohnersatzes nicht unterrichtet werden durfte.

Entgegen der Auffassung des Verbandsgemeindebürgermeisters waren die an die Presse weitergegebenen Informationen nicht öffentlich zugänglich. Weder in der Haushaltssatzung der Ortsgemeinde noch in dem entsprechenden Haushaltsplan war eine Position enthalten, die die von der VGV für den Ortsbürgermeister gezahlten Lohnersatzleistungen offen auswies. Vielmehr handelte es sich bei den jeweiligen Haushaltsansätzen um Pauschalbeträge, die eine exakte Zuordnung auf einzelne für bestimmte Zwecke zu zahlende Teilbeträge nicht ermöglichten. Aber auch die in einem Haushaltsjahr tatsächlich geflossenen Haushaltsmittel, die bezogen auf das einzelne Haushaltsjahr im Haushaltsplan der Ortsgemeinde ausgewiesen waren, gaben die an die Presse weitergegebene Information nicht wieder.

Angesichts der in § 6 Abs. 2 Nr. 2 LMG enthaltenen Regelung, wonach die grundsätzlich gegenüber den Medien bestehende Informationspflicht der Behörden eingeschränkt ist, wenn wie in diesem Fall Vorschriften über die Geheimhaltung entgegenstehen, war auch medienrechtlich die Weitergabe der Informationen an die Presse nicht zulässig.

19. Telekommunikation

19.1 Die Bedeutung der Telekommunikationstechnik für den Datenschutz

Die Telekommunikation ist in ihrer Bedeutung für die heutige Gesellschaft kaum zu überschätzen: Die Wirtschaft ist im nationalen und internationalen Bereich essentiell auf Telekommunikation angewiesen. Die Globalisierung, das Zusammenwachsen der Volkswirtschaften, beruht wesentlich auf den Möglichkeiten der weltweiten schnellen und unkomplizierten Kommunikation, die immer mehr mit Hilfe des Internets und der EDV-Technik erfolgt. Aber auch die privaten Kommunikationsbeziehungen werden mehr und mehr von diesen neuen Techniken bestimmt. Es ist die Rede davon, dass Telefonfestnetze bis zum Jahr 2011/2012 in Deutschland vollständig von Funknetzen und der Internettelefonie (Voice-over-IP) abgelöst sein werden. Das bedeutet, dass zunehmend ursprünglich flüchtige Informationen (nicht nur Verbindungs-, sondern auch Inhaltsdaten der Kommunikation) in digitaler Form gespeichert werden, was eine dauerhafte Aufbewahrung und eine relativ leichte Nutzbarkeit auch zu Zwecken, die über den eigentlichen Kommunikationszweck hinausgehen, zumindest ermöglicht. Damit geht eine Vielzahl von Datenschutzfragen einher (s. den 20. Tb., Tz. 19.1; zum Problembereich der TK-Vorratsdatenspeicherung s. Tz. 7.2.2).

19.2 Datenschutzkontrolle im TK-Bereich, Abstimmung der Aufsichtsbehörden

Die Zuständigkeiten für die Datenschutzkontrolle im TK-Bereich sind uneinheitlich und unübersichtlich. Der LfD ist für die datenschutzrechtliche Kontrolle zuständig, soweit öffentliche Stellen des Landes TK-Einrichtungen betreiben oder nutzen. In der Praxis dürfte jede dieser Stellen TK-Einrichtungen nutzen. Auch hier haben sich Fragen ergeben (s. unten Tz. 19.3 und 19.4).

Eine ganze Reihe von Eingaben hatte Fragen der Adressdatennutzung von Telefonkunden durch ihren deutschen Telekommunikationsdienstleister (sei es die Telekom oder andere Anbieter) zum Gegenstand. Diese Petenten musste der LfD sämtlich – unabhängig vom Bundesland, in dem sich der Sitz des Anbieters befand – an den BfDI verweisen. Dieser ist gem. § 115

Abs. 4 TKG für die datenschutzrechtliche Überwachung von Unternehmen zuständig, die „für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erheben, verarbeiten oder nutzen“.

Nicht ganz einfach ist in jedem Einzelfall die Entscheidung über die Zuständigkeit, wenn Gegenstand der Anfrage nicht die Datenverarbeitung durch einen TK-Dienstleister, sondern durch den Anbieter eines Telemediums ist. Ein Mediendienst ist jeder elektronische Informations- und Kommunikationsdienst, soweit er nicht ein Telekommunikationsdienst nach § 3 Ziff. 24 TKG, der ganz in der Übertragung von Signalen über Telekommunikationsnetze besteht, ein telekommunikationsgestützter Dienst nach § 3 Ziff. 25 des TKG oder Rundfunk nach § 2 Rundfunkstaatsvertrages ist (§ 1 Satz 1 TMG). In diesem Zusammenhang wird die Auffassung vertreten – die der LfD nicht teilt –, dass das Angebot von Internettelefonie ein Telemedium, nicht aber eine TK-Dienstleistung wäre. Für die Datenschutzüberwachung von Telemedien jedenfalls sind die örtlich und sachlich zuständigen Datenschutzaufsichtsbehörden der richtige Ansprechpartner (das ist die Landesdatenschutzaufsichtsbehörde, die für den Sitz des Telemediendienstleisters zuständig ist, bei öffentlich-rechtlichen Telemediendienstleistern der jeweilige Landesdatenschutzbeauftragte). Schließlich sind die Aufsichtskompetenzen bei Komplettanbietern (die aus einer Hand Telemedien- und TK-Dienstleistungen anbieten) und die Einordnung von Plattformbetreibern nach dem Rundfunkstaatsvertrag ungeklärt.

Angesichts der Zersplitterung der Datenschutzaufsicht in diesem Bereich einerseits und der oft vergleichbaren Datenschutzfragen andererseits kommt der Abstimmung der beteiligten Datenschutzaufsichtsbehörden eine besondere Bedeutung zu. Diese erfolgt insbesondere in folgenden Gremien:

- dem Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter dem Vorsitz der brandenburgischen Datenschutzbeauftragten und
- der AG Telekommunikation, Tele- und Mediendienste des „Düsseldorfer Kreises“ (der Datenschutzaufsichtsbehörden für den privaten Bereich) unter dem Vorsitz des Berliner Datenschutzbeauftragten.

Auf der internationalen Ebene ist in diesem Bereich eine Abstimmung ebenfalls unabdingbar. Sie erfolgt beispielsweise in

- der Internet Task Force der Art.-29-Gruppe (der Gruppe der in Europa tätigen Datenschutzbeauftragten) und
- der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation (der sog. „Berlin-Group“), die unter dem Vorsitz des Berliner Datenschutzbeauftragten tagt.

19.3 Die Nutzung von Internet und E-Mail in der Verwaltung

Internet und E-Mail gehören inzwischen zu den unverzichtbaren Arbeitsmitteln in der täglichen Verwaltungspraxis. Sie fördern insbesondere eine effiziente interne und externe Kommunikation sowie eine breite und beschleunigte Informationsbeschaffung. Ohne diese elektronischen Informations- und Kommunikationsdienste könnten heute zahlreiche Aufgaben der Verwaltung nicht mehr sach- und termingerecht erledigt werden. Die Nutzung von Internet und E-Mail am Arbeitsplatz führt allerdings nicht nur zur Erleichterung der täglichen Arbeit, sondern auch zu neuen Problemen im Verhältnis zwischen den Mitarbeitern und der Dienststelle. Diese (arbeits-)tägliche Problematik bildet einen Schwerpunkt der Beratungstätigkeit des LfD. Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu ihre Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz aktualisiert, das allen Beteiligten Hilfestellung bei den zu lösenden Fragen bieten soll.

In diesem Zusammenhang ist weiter die Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet zu erwähnen, die derzeit vom Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aktualisiert wird. Sie wird über das Internetangebot des LfD zugänglich sein.

19.4 ISDN-Leistungsmerkmal „Aufheben der Rufnummernunterdrückung“

Nach § 102 Abs. 1 und 2 TKG müssen die Anbieter von Telekommunikationsdienstleistungen ermöglichen, dass anrufende Teilnehmer die Anzeige ihrer Rufnummer fallweise oder dauerhaft unterdrücken können. Dem wird bei der ISDN-Telefonie durch das Leistungsmerkmal „Rufnummernunterdrückung“ (CLIR) entsprochen, das vom Anschlussinhaber entsprechend aktiviert werden kann.

Mit Blick auf die Besonderheiten bei Notrufstellen nimmt § 102 Abs. 6 i.V.m. § 108 TKG derartige Anschlüsse von der vorstehenden Regelung aus. In diesen Fällen wird für den jeweiligen Anschluss in der Vermittlungsstelle des Providers das Leistungsmerkmal „Aufheben der Rufnummernunterdrückung“ (CLIRO bzw. CLIRIGN) aktiviert. Dies führt dazu, dass die Nummer des anrufenden Teilnehmers beim angerufenen Anschluss (der Notrufstelle) angezeigt wird, auch wenn eine Rufnummernunterdrückung aktiviert wurde.

Datenschutzrechtlich kann dies problematisch sein, wenn hinter einem Anschluss, für den die Aufhebung einer Rufnummernunterdrückung eingerichtet wurde, weitere Nebenstellen existieren, die für sich betrachtet die Voraussetzungen des § 102 Abs. 6 TKG nicht erfüllen. Der LfD hat die diesbezügliche Praxis in Rheinland-Pfalz überprüft, insbesondere ging es dabei um die Frage, in welchem Umfang die Möglichkeit, eine etwaige Rufnummernunterdrückung aufzuheben, genutzt wird. Danach besteht an der TK-Anlage der Landeregierung keine Möglichkeit, bei ankommenden Anrufen eine ggf. aktivierte Rufnummernunterdrückung zu deaktivieren. Auch existieren im Bereich der Landesregierung einschließlich des Verfassungsschutzes keine Anschlüsse, für die grundsätzlich eine Aufhebung der Rufnummernunterdrückung aktiviert ist.

Dies ist lediglich bei den Erstalarmierungsstellen mit der Rufnummer 112 der Fall, d.h. den Leit- und Rettungsstellen, den Feuerwehreinsatzzentralen und Polizeidienststellen. Bei den Notrufabfragestellen der Polizei handelt es sich regelmäßig um eigens für diesen Zweck eingesetzte TK-Anlagen. Diese sind so konfiguriert, dass die Rufnummer bei einer gegebenenfalls erforderlichen Weiterleitung des Anrufs nicht übertragen wird.

19.5 Eingriffe in das Telekommunikationsgeheimnis zum Schutz des Urheberrechts

Das BMJ hat am 6.1.2006 den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, der in Umsetzung der „Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums“ (IPR-Enforcement-Richtlinie) den Schutz des Urheberrechts im nationalen Recht stärken soll. Der Gesetzentwurf gesteht den Rechteinhabern in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internetprovider auch über – durch das Fernmeldegeheimnis gem. Art. 10 GG geschützte – Daten ihrer Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbieter und Nutzer illegal kopierter Musik- oder Videodateien oder Software ermittelt werden können.

Gegen die Einräumung derartiger Auskunftsansprüche gegenüber unbeteiligten Dritten hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gewandt (71. Konferenz vom 16./17.3.2006 in Magdeburg, „Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht“, siehe Anlage 12). Danach lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Sie appelliert an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung privater wirtschaftlicher Interessen – zu verzichten. Es wäre nicht akzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden.

20. Medien

20.1 Das Telemediengesetz

Mit dem Telemediengesetz, das am 1.3.2007 in Kraft getreten ist, hat der Bund die Regelungen im Bereich der Tele- und der Mediendienste vereinheitlicht (BT-Drs. 16/3078: Gesetzentwurf nebst Begründung; Telemediengesetz vom 26. 2.2007, BGBl. I S. 179; vgl. 20. Tb., Tz. 20.1). Ein Mediendienst ist jeder elektronische Informations- und Kommunikationsdienst, soweit er nicht ein Telekommunikationsdienst nach § 3 Ziff. 24 des TKG, der ganz in der Übertragung von Signalen über Telekommunikationsnetze besteht, oder ein telekommunikationsgestützter Dienst nach § 3 Ziff. 25 des TKG oder Rundfunk nach § 2 Rundfunkstaatsvertrag ist (§ 1 Satz 1 TMG).

Die Datenschutzvorschriften, die bislang noch unterschiedlich für Tele- und Mediendienste im Teledienstedatenschutzgesetz bzw. im Mediendienstestaatsvertrag der Länder geregelt waren, wurden integriert. Dabei hat es keine wesentlichen Änderungen gegeben. Allerdings soll die bereits bestehende Befugnis der Diensteanbieter ausgeweitet werden, Daten ihrer Kunden (sog. „Bestandsdaten“) für Strafverfolgungszwecke an die zuständigen Stellen herauszugeben. Es dürfen auch Anfragen der Verfassungsschutzbehörden und Nachrichtendienste zu deren Aufgabenerfüllung beantwortet werden. Zum Schutz der Empfänger elektronischer Werbung wurden Regelungen aufgenommen, die das Verschleiern oder Verheimlichen des Absenders und des kommerziellen Charakters einer Werbe-E-Mail verbieten und ein Zuwiderhandeln mit einem Bußgeld belegen. Es wird weiter klargestellt, dass auch die öffentlichen Stellen, soweit sie Mediendienste betreiben, an die Anforderungen des Gesetzes gebunden sind (§ 1 Abs. 1 Satz 2 TMG). Dies betrifft insbesondere die Impressumspflicht. Für diese Pflicht besteht allerdings nach wie vor eine gewisse Rechtszersplitterung. Ergänzende Regelungen zur Impressumspflicht für Mediendienste finden sich auch im Rundfunkstaatsvertrag (§ 55 Rundfunkstaatsvertrag; vgl. hierzu Ott, Impressumspflicht für Webseiten, MMR 2007, S. 354).

Der LfD sieht es als seine Aufgabe an, auf die Einhaltung dieser Regelungen durch öffentliche Stellen hinzuwirken; er hat auch entsprechende Überprüfungen vorgenommen und gelegentlich Nachbesserungen angemahnt.

20.2 Befreiung von der Rundfunkgebührenpflicht wegen Bedürftigkeit

Nach den Bestimmungen des Rundfunkgebührenstaatsvertrages (RGebStV) werden u.a. die Empfänger bestimmter Sozialleistungen – insbesondere von Sozialhilfe, Grundsicherung, Sozialgeld und Arbeitslosengeld II – auf Antrag von der Rundfunkgebührenpflicht befreit. Nach § 6 Abs. 2 RGebStV hat der Antragsteller die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch Vorlage des – vollständigen – Sozialleistungsbescheides im Original oder in beglaubigter Kopie zentral bei der GEZ nachzuweisen. Damit erfährt die GEZ mehr, als sie für ihre Entscheidung zu wissen braucht.

Aufgrund der von den Datenschutzbeauftragten geäußerten Bedenken soll eine Änderung erfolgen. Künftig soll aufgrund einer entsprechenden Neufassung des § 6 Abs. 2 RGebStV dem Sozialleistungsempfänger eine Wahlmöglichkeit eingeräumt werden. Er soll die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht entweder durch Vorlage (lediglich) einer Bestätigung des Sozialleistungsträgers über die Gewährung und die Dauer der Sozialleistung (im Original) oder durch Vorlage des Sozialleistungsbescheides (im Original oder in beglaubigter Kopie) nachweisen können.

Die Rundfunkanstalten und die GEZ haben sich bereit erklärt, im Vorgriff auf diese staatsvertragliche Regelung entsprechende Bestätigungen anzuerkennen. Es ist aber darauf hinzuweisen, dass eine Verpflichtung aller Sozialleistungsbehörden zur Ausstellung dieser Bestätigungen im Rundfunkgebührenstaatsvertrag (aus Gründen der insoweit mangelnden Rechtssetzungsbefugnis der Vertragspartner) nicht begründet werden kann. Als Vorsitzender der Rundfunkkommission hat deshalb der Ministerpräsident des Landes Rheinland-Pfalz auch im Namen der Rundfunk- und der Landesdatenschutzbeauftragten bei der Bundesagentur für Arbeit und bei den betroffenen kommunalen Spitzenverbänden für die Bestätigungslösung geworben. Es bleibt eine Aufgabe des LfD, die betroffenen Sozialleistungsträger zur Mitwirkung zu bewegen.

20.3 Die Datenschutzaufsicht im Medienbereich

Die im Lande ansässigen bzw. tätig werdenden öffentlich-rechtlichen Rundfunkanbieter sind das ZDF sowie der SWR. Sie unterliegen nicht der Datenschutzaufsicht durch den LfD. Dies beruht auf den Regelungen im Landesdatenschutzgesetz von Baden-Württemberg (§ 38) sowie auf dem ZDF-Staatsvertrag (§ 18), wonach für beide Anstalten eigene Rundfunkdatenschutzbeauftragte die Datenschutzkontrolle an der Stelle des LfD wahrnehmen. Sie sind innerhalb ihrer jeweiligen Anstalten unabhängig. Für Eingaben, die die GEZ betreffen, übt der Datenschutzbeauftragte des SWR die alleinige Zuständigkeit für die Rundfunknutzer seines Sendebereichs aus.

Für private Rundfunkanbieter ist die Kontrolle durch die jeweilige Landesmedienanstalt sowie durch die für private Stellen zuständige Datenschutzaufsichtsbehörde (in Rheinland-Pfalz die ADD) wahrzunehmen. Landesmedienanstalt in Rheinland-Pfalz ist die „Landeszentrale für Medien und Kommunikation (LMK)“, Turmstraße 10, 67059 Ludwigshafen, Internet: http://www.lmk-online.de/ (die frühere „Landeszentrale für private Rundfunkveranstalter“; s. Herb, Die Struktur der Datenschutzkontrollstellen in der Bundesrepublik, Zeitschrift für Urheber- und Medienrecht 2004, 530). Anbieter von Telemedien unterliegen der Datenschutzaufsicht der Aufsichtsbehörden der Länder. Die Länder bleiben auch für die Internetprovider im Bereich ihrer Internetangebote außerhalb des Bereichs der „Übertragung von Signalen über Telekommunikationsnetze“ zuständig. Inhaltlich richten sich die datenschutzrechtlichen Prüfmaßstäbe nach dem Landesmediengesetz, dem TMG, dem Rundfunkstaatsvertrag (bzw. dem ZDF-Staatsvertrag) und nach den Datenschutzgesetzen des Bundes bzw. des Landes. Nach dieser Rechtslage hat der LfD also nur Zuständigkeiten für die Medien, die von öffentlichen Stellen des Landes (außerhalb der öffentlich-rechtlichen Rundfunkanstalten und der Kirchen) verantwortet werden.

Allerdings besteht ein enger Kontakt zwischen dem LfD und den Datenschutzbeauftragten von ZDF (Herrn Christoph Bach) und des SWR (Herrn Prof. Armin Herb). Das gemeinsame Anliegen besteht darin, im Interesse des Datenschutzes unterschiedliche Wertungen vergleichbarer Sachverhalte – bei voller Wahrung der Unabhängigkeit der Beteiligten – zu vermeiden. Dies ist bislang gelungen. Wie intensiv – und unabhängig auch gegenüber den Anstalten – die Aufgabe der Datenschutzkontrolle durch die Rundfunkdatenschutzbeauftragten wahrgenommen wird, lässt sich deren Tätigkeitsberichten bzw. Internetauftritten entnehmen (http://www.swr.de/; http://www.unternehmen.zdf.de/).

20.4 Individuelle Erfassung des Medienkonsumverhaltens durch Pay-TV-Angebote

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit

personenbezogenen Smartcards möglich sein soll. Die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu am 8.-9.3.2007 in Erfurt eine Entschließung mit dem Titel: „Anonyme Nutzung des Fernsehens erhalten!“ verabschiedet, die an das Prinzip der Datenvermeidung erinnert und dazu auffordert, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln (s. Anlage 21).

21. Technisch-organisatorischer Datenschutz

21.1 Kontroll- und Beratungstätigkeit, Schulungen, Kooperationen

Im Berichtszeitraum sind in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung in 88 Fällen örtliche Feststellungen und Beratungen unter technisch-organisatorischen Gesichtspunkten erfolgt, u. a. bei folgenden Stellen:

- Staatskanzlei
- Ministerium des Innern und für Sport
- Justizministerium
- Finanzministerium
- Ministerium für Arbeit, Soziales, Gesundheit, Familie und Frauen
- Ministerium für Bildung, Wissenschaft, Jugend und Kultur
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau
- Universitätsklinikum
- Landeskriminalamt
- Polizeipräsidien
- Polizei-/Kriminalinspektionen
- Zentralstelle für Polizeitechnik
- Landesbetrieb Daten und Information
- Zentralstelle für IT-Management, Multimedia, E-Government und Verwaltungsmodernisierung
- Statistisches Landesamt
- Arbeitsgemeinschaften nach § 44 b SGB II
- Kassenärztlichen Vereinigung Rheinland-Pfalz
- Landesmedienzentrum
- Landesamt für Jugend, Soziales und Versorgung
- Krebsregister
- Kinderkrebsregister
- Landespsychotherapeutenkammer
- Gesellschaft für Kommunikation und Wissenstransfer
- Kommunalverwaltungen
- Struktur- und Genehmigungsdirektion
- Oberfinanzdirektion / Zentrale Besoldungs- und Versorgungsstelle
- Finanzämter
- Sparkassen

Ergänzt wurden diese örtlichen Feststellungen und Beratungen durch 33 Informationsbesuche, bei denen zumeist die Klärung des technischen Verfahrensstands im Vordergrund stand. Kontrollen erfolgten sowohl in Form allgemeiner Prüfungen als auch anlassbezogen bzw. unter ausgewählten Gesichtspunkten. Mit Blick auf die zunehmende Verlagerung von Verwaltungsleistungen ins Internet hat der LfD begonnen, Online-Kontrollen durchzuführen und die Internetangebote und -portale von Verwaltungen auf ihre Übereinstimmung mit datenschutzrechtlichen Vorschriften zu überprüfen. In gleichem Zusammenhang wurden Kontrollen der Sicherheit von Webanwendungen der Verwaltungen durchgeführt. Dies ist zum Teil mit Unterstützung einschlägiger Beratungsunternehmen erfolgt. Breite und Tempo der technischen Entwicklung in diesem Bereich erfordern teils spezielle Kenntnisse und (kommerzielle) Software, die beim LfD vorzuhalten mit unverhältnismäßigem Aufwand verbunden wäre. Der LfD greift daher bei besonderen Fragestellungen auf entsprechende Dienstleister zurück; dies hat sich im Berichtszeitraum wiederholt als sinnvoll erwiesen. Die bisherige Praxis der Verwaltung, den LfD im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder der Erstellung von Sicherheitskonzepten zu beteiligen, wurde beibehalten. Insbesondere bei der Einführung zentraler Verfahren wird im Regelfall frühzeitig die Abstimmung mit dem LfD gesucht. Die Schulungsaktivitäten wurden im bisherigen Umfang fortgeführt.

Mit dem Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau hat der LfD eine Kooperation vereinbart. Die Zusammenarbeit betrifft vor allem die gemeinsame Betreuung von Abschlussarbeiten und Projekten. Im einem ersten Schritt wurden hierzu Themenbereiche definiert, die im Interesse beider Kooperationspartner liegen, wie Identitätsmanagement, Implementierung datenschutzfreundlicher Technologien, Pseudonymisierungskonzepte, IT-Sicherheitsmanagement oder die technischen Möglichkeiten zur Umsetzung der Datenschutzrechte Betroffener. Im Berichtszeitraum haben drei Diplom- bzw. Masterarbeiten entsprechende Themenstellungen aufgegriffen.

21.2 Allgemeine technisch-organisatorische Aspekte

21.2.1 IT-Sicherheit in der Landesverwaltung

Unter Mitarbeit des LfD wurden im Jahr 2003 von einer Arbeitsgruppe des IT-Ausschusses der Landesregierung Leitlinien zur Sicherheit beim Einsatz der Informationstechnik in der Landesverwaltung erarbeitet. Diese fußen auf den Empfehlungen des BSI zum IT-Grundschutz. Die Sicherheitsleitlinien wurden im Ministerrat beschlossen und als Rundschreiben der Landesregierung veröffentlicht (Planung und Realisierung der IT-Sicherheit in der Landesverwaltung Rheinland-Pfalz, MinBl. vom 4. Juni 2003, S. 327).

Die in den Sicherheitsleitlinien angesprochenen Punkte wurden bislang erst in Teilen umgesetzt. Ein vergleichsweise hohes Sicherheitsniveau existiert für die vom LDI betreuten IT-Strukturen, d.h. das Landesdaten- und Kommunikationsnetz (rlp-Netz), den zentralen Internetübergang der Landesverwaltung und das zentrale Rechenzentrum. In einzelnen Verwaltungsbereichen ist nach den Erkenntnissen des LfD das Sicherheitsniveau jedoch unterschiedlich. Strukturierte Schutzbedarfsanalysen oder auf der Grundlage der BSI-Empfehlungen erstellte Sicherheitskonzepte stellen die Ausnahme dar. Sicherheitsmaßnahmen werden häufig nur punktuell getroffen, ein IT-Sicherheitsmanagement als Geschäftsprozess existiert nur in Einzelfällen. Der Aufbau einer in den Sicherheitsleitlinien geforderten Informationsplattform IT-Sicherheit für die Landesverwaltung steht noch aus.

Der LfD hat daher gegenüber dem ISM auf die Notwendigkeit hingewiesen, das Thema IT-Sicherheit in der Landesverwaltung erneut aufzugreifen und die Umsetzung der im o.g. Rundschreiben angesprochen Punkte angemahnt. Erste Gespräche hierzu wurden geführt.

21.2.2 Anforderungen an Verfahrenstests mit Echtdaten

Im Berichtszeitraum hat sich wiederholt die Situation ergeben, dass im Zusammenhang mit der Einführung oder Umstellung von IT-Verfahren für notwendige Verfahrenstests auf Echtdaten zurückgegriffen werden sollte. Von Bedeutung ist dies insbesondere in Fällen, in denen private Unternehmen mit der Verfahrensentwicklung beauftragt sind. Aus datenschutzrechtlicher Sicht sind im Rahmen der Verfahrensentwicklung vorgesehene Tests grundsätzlich anhand geeigneter Testdaten durchzuführen. Die Verwendung von Echtdaten kommt nur insoweit in Betracht, als die zu testenden Sachverhalte mit den Testdaten nicht hinreichend verlässlich erfasst werden oder der Aufwand zu deren Erzeugung in erforderlichem Umfang und Ausprägung außer Verhältnis steht.

Vor einer Nutzung von Echtdaten sind die Möglichkeiten zu prüfen, diese zu anonymisieren oder zu pseudonymisieren. Im Einzelfall kann dies jedoch auf Probleme stoßen, z.B. dort, wo gerade die Vielfalt von Namensausprägungen Gegenstand eines Tests auf korrekte Verarbeitung sein soll. Für diese Fälle sollten die personenbezogenen Originaldaten dadurch „verschleiert“ werden, dass die für eine Zuordnung der Datensätze zu einer Person nutzbaren Feldinhalte irreversibel durch zufällig ausgewählte Ausprägungen des Gesamtbestands ausgetauscht werden. Namensausprägungen, die weniger als fünfmal vorkommen, gehen dabei nicht in den zu erzeugenden Datenbestand ein. Etwaige Freitextfelder werden durch neutrale Texte ersetzt; ähnliches gilt für sonstige Dateianhänge. Nach Einschätzung des LfD sind bei ordnungsgemäßer Umsetzung anhand der nicht ersetzten Inhalte eines Datensatzes mit vertretbarem Aufwand keine konkreten Personen bestimmbar, so dass den Vorgaben des § 3 Abs. 7 LDSG entsprochen wird.

Von datenschutzrechtlicher Bedeutung ist allerdings, dass es sich bei den für die Ersetzung verwendeten Namen oder Straßenbezeichnungen um Angaben aus dem Originalbestand und damit nicht um neutrale Inhalte handelt. Je nach Umstand können sie Hinweise darauf geben, dass Personen aus einer eingrenzbaren Gruppe betroffen waren. Soweit für etwaige Auftragnehmer entsprechende Vereinbarungen getroffen werden, ist dies aus Sicht des LfD jedoch hinnehmbar.

Der Landesbeauftragte hat hierzu folgende Empfehlungen ausgesprochen:

- Verfahrenstests mit Echtdaten sind nach § 4 Abs. 5 LDSG als Datenverarbeitung im Auftrag anzusehen. Ihnen sind die Anforderungen nach § 4 Abs. 1 bis 4 LDSG bzw. die entsprechenden bereichsspezifischen Regelungen (z.B. § 80 SGB X) zugrunde zu legen.
- Die bereitgestellten Daten dürfen nur für Testzwecke verwendet werden. Diese sind inhaltlich festzulegen und zeitlich zu beschränken. Eine darüber hinausgehende Nutzung ist unzulässig.
- Die Echtdaten sind nur den an den Tests beteiligten Personen zugänglich zu machen. Diese sind zuvor nach § 8 LDSG auf die Wahrung des Datengeheimnisses zu verpflichten.
- Sollen die Daten an nicht-öffentliche Stellen abgegeben werden, sind, um die Anwendbarkeit strafrechtlicher Bestimmungen wie bei Amtsträgern zu gewährleisten (§ 203 StGB), die betroffenen Mitarbeiter des Auftragnehmers nach dem Verpflichtungsgesetz für den öffentlichen Dienst besonders zu verpflichten und Geheimhaltungserklärungen vorzusehen.
- Die zur Verfügung gestellten Daten einschließlich etwaiger Kopien sind nach Abschluss der Tests zu löschen. Überlassene Datenträger sind zurückzugeben. Die erfolgte Löschung bzw. die erfolgte Vernichtung von Datenträgern ist durch den Auftragnehmer zu bestätigen.

21.2.3 Sicherheit von Webanwendungen

Über sog. Webanwendungen werden in zunehmendem Maß Verwaltungsleistungen über das Internet zugänglich gemacht, die bislang in verwaltungsinternen Verfahren erbracht wurden. Diese Öffnung für Zugriffe aus dem Internet führt zu neuen Angriffsszenarien, auf die vorhandene Sicherheitsmaßnahmen vielfach nicht ausgerichtet sind. Im Rahmen des Aktionsplans „E-Government“ der Landesregierung werden zunehmend auch in Rheinland-Pfalz internetbasierte Zugänge zu Fachverfahren der Verwaltungen eröffnet. Der LfD hat parallel zu dieser Entwicklung seine Online-Kontrollen intensiviert.

Dabei hat sich wiederholt die Verwundbarkeit gegenüber unbefugten Datenzugriffen, Datenveränderungen und Beeinträchtigungen der Verfügbarkeit oder Funktionsfähigkeit von Verfahren ergeben, in einem Fall war ein im Länderverbund entwickeltes Verfahren betroffen. Kritisch ist in diesem Zusammenhang anzumerken, dass die vorliegende Schwachstelle im Entwicklungsverbund bekannt war, die Notwendigkeit geeigneter, landesseitiger Vorkehrungen bei der Übernahme des Verfahrens durch Rheinland-Pfalz jedoch nicht thematisiert wurde.

U.a. folgende beispielhafte Verfahren waren von Schwachstellen betroffen:

- Gemeinsames Internetangebot von Stellen mehrerer Bundesländer.
  Die Stellen mehrerer Bundesländer bedienten sich für den Betrieb ihres Internetangebots eines von der koordinierenden Verwaltung beauftragten privaten Dienstleisters. Eine Klärung der in administrativer Hinsicht zu erbringenden Betriebsleistungen war nicht erfolgt.

  Aufgrund fehlerhaft gesetzter Zugriffsrechte bestand die Möglichkeit, über das Internet auf Protokolldaten zuzugreifen. Der unbefugte Zugriff gründete darauf, dass eine manipulierte Internetadresse angegeben und damit aus dem für die Benutzer vorgesehenen Bereiche ausgebrochen werden konnte (sog. Directory-Traversal). Im Ergebnis war das Herunterladen von Zugriffsdaten im Gesamtvolumen von etwa 300 MB/1.600 Druckseiten möglich. Betroffen waren die Daten mehrerer Länder sowie des Bundes.

- Internetbasierte Registeranwendung
  Bei einer Registeranwendung war es aufgrund der fehlenden Filterung der benutzerseitigen Eingaben möglich, ohne gültige Benutzerkennung und ohne Kenntnis eines Passworts auf die Registerdaten zuzugreifen. Durch die Eingabe einer bestimmten Zeichenfolge in der Ameldemaske des Verfahrens wurde die vorgesehene Passwortprüfung ausgehebelt und der Zugang zur Registerdatenbank eröffnet (sog. SQL-Injection).

- Mailserver mit internetbasiertem Zugang (Outlook Web Access)
  Aufgrund der mangelhaften Konfiguration des Systems konnten erfolgreich sog. „Wörterbuch- bzw. Brute-Force-Attacken“ durchgeführt werden. Dabei wurden automatisiert und systematisch eine Vielzahl möglicher Kombinationen aus Benutzerkennungen und Passworten ausprobiert. Auf diese Weise wurden in ca. 15 Fällen gültige Zugangsdaten ermittelt. Dadurch war es möglich, auf die Postein- und -ausgangsfächer zuzugreifen und unter vertrauenswürdigen Absenderadressen vorgetäuschte E-Mails zu versenden. Weiterhin war es grundsätzlich möglich, einen administrativen Zugang und damit die Kontrolle über das Verfahren zu erhalten.

Bedeutsam ist in diesem Zusammenhang, dass die jeweiligen Schwachstellen zumeist in den Anwendungen selbst bestanden und damit von gängigen Sicherheitsvorkehrungen auf Netzebene (Adress-, Dienste- und Portfilterung, Netzsegmentierung) nicht abgedeckt wurden. Weitere Ursachen lagen im Bereich der Administration bzw. Konfiguration der Systeme. Insbesondere dort, wo kein systematisches Härtungs- und Überwachungskonzept verfolgt wurde, wurden Angriffe erleichtert. Ein grundsätzliches Problem war nach den Erkenntnissen des LfD, dass benutzerseitige Eingaben vielfach ungefiltert bzw. unzureichend gefiltert an die jeweilige Anwendung weitergereicht wurden und über die Eingabe geeigneter Zeichenfolgen vorhandene Sicherheitsmechanismen umgangen werden konnten.

Es hat sich als Problem erwiesen, dass das Sicherheitsniveau der Fachverfahren der Einwirkung des technischen Betreibers weitgehend entzogen ist. Dieser hat – bei Kenntnis der Schwachstellen – u.U. begrenzte Möglichkeiten diese auszugleichen. Entsprechende Vorkehrungen müssen jedoch primär im Rahmen der Verfahrensentwicklung getroffen werden und liegen damit in erster Linie in der Verantwortung der die Entwicklung beauftragenden Verwaltung. Durch betriebsseitige Sicherheitsmaßnahmen oder Sicherheitsmechanismen der jeweiligen Verfahrensplattform können Defizite nur zum Teil ausgeglichen werden.

Die Feststellungen zeigen, dass bei E-Government-Anwendungen Sicherheitsaspekte gezielt auf Anwendungs-, System- und Netzebene zu betrachten sind. Die Öffnung von Verwaltungsverfahren für Zugriffe aus dem Internet führt zu Angriffsszenarien, für welche netzseitig getroffene Sicherheitsmaßnahmen vielfach nicht ausgelegt sind. Nach Auffassung des LfD sollte daher im Rahmen der Verfahrensentwicklung eine Risikobetrachtung durchgeführt werden, die die Berücksichtigung entsprechender Sicherheitsmaßnahmen in der Entwicklung oder für den Betrieb gewährleistet. Vergleichbar der Untersuchung zur E-Government-Tauglichkeit von Verwaltungsverfahren, wie Sie im Rahmen des Aktionsplans der Landesregierung erfolgt, sollten auch die notwendigen Sicherheitsaspekte methodisch und entwicklungsbegleitend bedacht werden (Pflichtenheft „Verfahrenssicherheit“, Sicherheitsevaluation, E-Government-Leitlinien).

Die Öffnung von Verwaltungsverfahren gegenüber dem Internet zwingt dazu, Sicherheitsaspekte bereits frühzeitig im Rahmen der Anwendungsentwicklung zu berücksichtigen; eine nachgelagerte Filterung während des Betriebs ist vielfach nur bedingt in der Lage, Angriffen auf Anwendungsebene vorzubeugen.

21.2.4 Deutsches Verwaltungsdienste-Verzeichnis (DVDV)

Das DVDV bildet eine fach- und ebenenübergreifende Infrastrukturkomponente für das E-Government in Deutschland. Grundlage des DVDV ist ein Verzeichnisdienst, in dem Behörden des Bundes und der Länder mit ihren Diensten aufgenommen werden können. Auskunftssuchende und Nutzer des DVDV sind Fachverfahren, die über die im DVDV enthaltenen Angaben die jeweiligen Dienste ansprechen können. Das DVDV wird durch die BIT betrieben.

Die Datenpflege der DVDV-Einträge obliegt den einzelnen Ländern. Sie erfolgt über entsprechende Pflegeclients direkt auf dem Bundesmaster bei der BIT. Die Abfrage von DVDV-Einträgen erfolgt landesseitig jeweils bei einem Landesmaster, dessen Datenbestand sich über eine Teilreplikation des Bundesmasters ergibt. In der gegenwärtigen Anlaufphase ist auf dem DVDV-Bundesmaster je beteiligtem Land eine Zugangskennung eingerichtet, eine weitere Differenzierung nach zugreifenden Stellen innerhalb der Länder erfolgt nicht. Soweit daher auf Landesebene mehrere Stellen DVDV-Einträge pflegen, können diese schreibend auch auf die Einträge der jeweils anderen Stellen zugreifen. Die Zahl der unter einer Landeskennung zugreifenden Stellen richtet sich meist nach der Anzahl der im Land eingesetzten Intermediäre. Aufgrund der bestehenden Strukturen in Rheinland-Pfalz kommt hier lediglich ein Intermediär zum Einsatz, der sowohl von staatlicher als auch von kommunaler Seite genutzt wird. Die Vereinbarung zur Datenpflege sieht vor, dass die DVDV-Einträge von je einer Stelle für das Land bzw. die Kommunen gepflegt werden.

Hinsichtlich der diskutierten Datenschutz- und Sicherheitsaspekte ist das Verwaltungsdiensteverzeichnis aus Sicht des LfD – vergleichbar dem Domain Name Service – als Strukturkomponente zu bewerten, die grundsätzlich keine personenbezogenen Daten bereithält. Mit Blick auf bestimmte Szenarien, bei welchen die Kompromittierung derartiger Komponenten Grundlage weitergehender Angriffe ist, betont er gleichwohl die Notwendigkeit, eine angemessene Zugangskontrolle und Nachvollziehbarkeit der DVDV-Nutzung zu gewährleisten. Die dauerhafte Nutzung einer Sammelkennung je Land erscheint in diesem Zusammenhang, jedenfalls bei einer größeren Zahl darunter agierender Stellen, problematisch.

21.2.5 Nutzung von Google-Toolbar und Google-Desktop, Löschung von Google-Einträgen

Die vom Suchmaschinenbetreiber Google angebotenen Dienste waren mehrfach Gegenstand von Anfragen an den LfD. Dabei wurde insbesondere die datenschutzrechtliche Bewertung der „Google-Toolbar“ bzw. des Programms „Google-Desktop“ nachgefragt.

Über die „Google-Toolbar“ wird der Zugriff auf verschiedene Zusatzdienste wie Übersetzungen, Rechtschreibprüfung, Nachrichtensuche oder Sicherheitshinweise ermöglicht. Bei einem Teil der Funktionen werden dabei über die üblicherweise bei Google-Anfragen übertragenen Informationen (URL, Suchparameter, Datum/Uhrzeit) hinausgehende Daten an Google übermittelt (z.B. über die aktuell im Internet besuchte Seite). Diese werden zur Individualisierung mit einer für die jeweilige Installation eindeutigen „Anwendungsnummer“ verbunden. Woraus sich diese im Einzelnen zusammensetzt, ist dem LfD nicht bekannt; in anderen Fällen werden derartige Identifikationskennzeichen häufig aus bestimmten Systemparametern gebildet, um das jeweilige Endgerät individuell zu kennzeichnen. Diese können u.U. einen Personenbezug aufweisen (z.B. bei Verwendung einer namensbezogenen UserID oder der PC-Bezeichnung des Benutzers). Eine Zuordnung der an Google übertragenen Informationen zur jeweiligen Verwaltung ist aus Sicht des LfD jedoch in der Praxis nicht zu vermuten, da über den zentralen Internetzugang des LDI eine Umsetzung auf die IP-Adresse des Landesnetzes erfolgt und damit die nutzende Stelle verborgen wird. Ein Personenbezug zum jeweiligen PC-Nutzer kann sich allerdings ergeben, wenn Funktionen der Toolbar im Zusammenhang mit einem für einen Google-Dienst eingerichteten „Google-Konto“ genutzt werden. Die Toolbar-Funktionen, bei denen zusätzliche Informationen übermittelt werden, lassen sich deaktivieren bzw. sind im Rahmen der Standardinstallation zunächst ausgeschaltet, so dass eine entsprechende Steuerungsmöglichkeit besteht.

Datenschutzrechtliche Gesichtspunkte stehen einer Nutzung der Toolbar damit nicht grundsätzlich entgegen. Deren Konzept ermöglicht es jedoch, weitere Dienste einzubinden. Deswegen sollte sich die Beurteilung nicht allein auf die grundsätzliche Nutzung, sondern auch auf die jeweils genutzten Funktionen erstrecken. Hierbei sind diejenigen aus Datenschutzsicht problematisch, in deren Rahmen Informationen über gespeicherte Inhalte an Dritte übermittelt werden. Dies ist beispielsweise bei einzelnen Funktionen der Software „Google-Desktop“ der Fall, bei denen die auf dem PC bzw. im LAN vorhandenen Dateien mit ihrem Inhalt indiziert werden und dieser Suchindex bei Google gespeichert wird. Soweit diese oder vergleichbare Funktionen genutzt werden, begegnet dies datenschutzrechtlichen Bedenken.

Soweit es von der jeweiligen Verwaltung nicht grundsätzlich installiert oder zugelassen ist, ist eine Installation der Toolbar eine Veränderung der Softwarekonfiguration und wäre daher nur mit Zustimmung der IT-Betreuung zulässig. Aufgrund der technischen Gegebenheiten ist es in der Praxis zwar nur bedingt möglich sicherzustellen, dass dies verlässlich eingehalten wird. Um unerwünschte Datenabflüsse zu vermeiden, sollte aus datenschutzrechtlicher Sicht daher von einer generellen Freigabe der „Google-Toolbar“ bzw. vergleichbarer Erweiterungen abgesehen werden. Eine Installation sollte nur im Einzelfall, auf Anfrage und in Absprache mit der IT-Betreuung erfolgen. Dadurch wird gewährleistet, dass u.U. problematische Funktionen deaktiviert werden.

Nicht selten haben sich Bürger mit der Frage an den LfD gewandt, wie sie es erreichen können, mit ihren Internet-Fundstellen von Google nicht mehr angezeigt zu werden. Obwohl der LfD für Google keine Kontrollzuständigkeit besitzt, hat er dennoch im Rahmen seiner allgemeinen Pflicht, die Bürger über ihre Datenschutzrechte aufzuklären, dazu allgemein wie folgt geantwortet:

Da Google nur die Angebote fremder Anbieter auswertet und sie nachweist, muss ein Betroffener sich für Löschungen von Einträgen unmittelbar an den Verantwortlichen der Website (den Domaininhaber bzw. den dortigen administrativen Verantwortlichen) wenden, der über die Nameserver herauszufinden ist. Man sollte sich also zunächst unmittelbar an den Inhaber der jeweiligen Domain mit dem Anliegen auf Löschung des unzutreffenden oder aus sonstigen Gründen unzulässigen Inhalts wenden. Falls dies nicht zufriedenstellend erfolgt, sollte der für den Domain-Inhaber zuständige Datenschutzbeauftragte um Hilfe ersucht werden. Der verantwortliche Ansprechpartner einer Domain kann bei de-Domains über http://www.denic.de/de/whois/index.jsp gefunden werden. Der administrative Ansprechpartner (admin-c) ist die vom Domaininhaber benannte natürliche Person, die als sein Bevollmächtigter berechtigt und gegenüber DENIC auch verpflichtet ist, sämtliche die Domain betreffenden Angelegenheiten verbindlich zu entscheiden. Bei .com- und anderen Domains hilft beispielsweise http://www.who.is/.

Bei Cache-Speicherungen, die auch nach der Löschung im originalen Angebot für eine gewisse Zeit durch Google weiter angezeigt werden, ist ebenso zu verfahren: Die Löschung auch dieser Inhalte sollte zunächst ebenfalls über den Verantwortlichen veranlasst werden, der die Information ins Netz gestellt hatte. Dieser müsste sich an Google wenden. In Ausnahmefällen – z.B. bei mangelnder Mitwirkungsbereitschaft dieser Stelle – kann auch eine unmittelbare Löschung über folgenden Weg versucht werden: http://www.google.de/intl/de/remove.html.

Da Google Deutschland selbst keine verantwortliche speichernde Stelle ist, besteht im Fall von verbleibenden Problemen noch die Möglichkeit, die für das kalifornische Unternehmen Google zuständige kalifornische Datenschutzinstitution anzurufen. Dies ist möglich über http://www.privacyprotection.ca.gov/ Office of Privacy Protection – California Department of Consumer Affairs, die Website der kalifornischen Datenschutzbehörde (Englisch).

21.2.6 Baustein „Datenschutz“ in den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik

Das BSI stellt mit den BSI-Standards und den IT-Grundschutzkatalogen (ehemals IT-Grundschutzhandbuch) anerkannte Hilfsmittel bereit, mit denen für typische Einsatzszenarien der Informationstechnik ein angemessenes Sicherheitsniveau realisiert werden kann. Aufgrund der zum Teil engen Verflechtung datenschutzrechtlicher Anforderungen mit den Sicherheitszielen der Informationstechnik, etwa im Bereich der technisch-organisatorischen Datenschutzmaßnahmen, haben die Datenschutzbeauftragten vorgeschlagen, die Grundschutzkataloge um einen Baustein „Datenschutz“ zu ergänzen, der die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und die Verbindung zur IT-Sicherheit im IT-Grundschutz aufzeigt.

In Abstimmung mit den für die Datenschutzaufsicht im nicht öffentlichen Bereich zuständigen Stellen und dem BSI haben die Datenschutzbeauftragten des Bundes und der Länder einen entsprechenden Baustein erstellt. Dieser soll in die nächste Version der IT-Grundschutzkataloge aufgenommen werden.

Der Baustein folgt im Aufbau der Systematik der Grundschutzkataloge, indem er mögliche Gefährdungen für den Datenschutz beschreibt und geeignete Maßnahmen vorschlägt, um diesen zu begegnen. Der Baustein kann im Internet-Angebot des LfD unter http://www.datenschutz.rlp.de/ aus der Rubrik „Materialien zum Datenschutz“ abgerufen werden.

21.2.7 Versand von Patientenunterlagen per Telefax

Ein Privatmann hatte sich mit dem Hinweis an die Bezirksärztekammer gewandt, dass er mehrfach Telefaxe eines Klinikums mit Patientenunterlagen erhalten und es sich dabei offenkundig um Irrläufer gehandelt habe (z.B. Arztbriefe, Diagnosen). In der Folge konnten trotz einzelner organisatorischer Maßnahmen die Fehlsendungen nicht unterbunden werden. In mehreren Fällen gingen bei dem Petenten weiterhin Telefaxe ein, die an eine Rehabilitationsklinik in Hessen gerichtet waren. Nach seiner Auskunft habe er in den zurückliegenden Jahren ca. fünfzig solcher Zusendungen erhalten.

Die Feststellungen des LfD ergaben, dass der fehlerhafte Versand auf wiederholten Fehleingaben bei der Anwahl des Empfängers beruhte. Durch versehentliches Weglassen der führenden Null wurde statt einer Fernverbindung jeweils eine Verbindung im Ortsnetz hergestellt. Diese wiederum führte zu dem Faxanschluss des Petenten. Trotz der wiederholen Hinweise des Petenten an das Klinikum ist eine Unterrichtung der Absender unterblieben. Dadurch ist es in der Folge zu weiteren Fehlsendungen gekommen. Wirksame Maßnahmen wurden erst über ein Jahr nach den Hinweisen und erst nach der Einschaltung des LfD ergriffen. Aufgrund dieser Tatsache, wegen der Sensibilität der betroffenen Daten und der wiederholten Irrläufer hat der LfD dies nach § 25 Abs. 1 LDSG beanstandet. Die Klinikleitung hat daraufhin zeitnah reagiert und eine Sperre der Anschlussnummer des Petenten in der Nebenstellenanlage des Klinikums eingerichtet, wodurch weitere Fehlsendungen verlässlich ausgeschlossen wurden. Nichtsdestoweniger ist der Versand von Patientenunterlagen per Telefax aus Sicht des LfD problematisch und muss auf dringliche Einzelfälle beschränkt werden und mit der gebotenen Sorgfalt erfolgen. Hierzu zählt u.a., dass:

- die Anschlussnummern der am häufigsten per Telefax angeschriebenen Stellen erhoben und in den Faxgeräten fest eingegeben werden (Kurzwahlfunktion),
- an den Telefaxgeräten deutliche Hinweise angebracht werden, dass beim Versand an Stellen außerhalb der Einrichtung eine bestimmte Ziffer (üblicherweise die 0) der eigentlichen Rufnummer voranzustellen ist und
- zu prüfen ist, ob bei den empfangenden Stellen anstelle eines allgemeinen Faxanschlusses separate Geräte genutzt werden können. Dadurch wird vermieden, dass Telefaxe mit sensiblen Informationen in Bereiche geschickt werden, die allgemein zugänglich sind.

21.2.8 OSCI-Standard

In modernen E-Government-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht ein Protokollstandard zur Verfügung, der die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) bietet und eine rechtsverbindliche Transaktion zwischen den Teilnehmern einer elektronischen Kommunikation sicherstellt.

Werden E-Government-Anwendungen auf der Basis des OSCI-Standards Version 1.2 entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit angemessen erfüllen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung

vom 15.12.2005 (Anlage 8) die vom Koordinierungsausschuss Automatisierte Datenverarbeitung, dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung begrüßt, in E-Government-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um eine den datenschutzrechtlichen Anforderungen entsprechende Ende-zu-Ende-Sicherheit zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Gegenwärtig erfolgt die Entwicklung des OSCI-Standards in der Version 2.0. Diese soll nach Auskunft des Bundesinnenministeriums erweiterte Einsatzszenarien berücksichtigen, um eine größere Einsatzbreite des Standards zu erzielen. Vorliegende Informationen deuten darauf hin, dass in bestimmten Szenarien von dem aus datenschutzrechtlicher Sicht bewährten Konzept des „doppelten Briefumschlags“ abgewichen werden soll. Der Arbeitskreis Technik der Datenschutzbeauftragten hat in diesem Zusammenhang seine Mitarbeit bei der Weiterentwicklung angeboten. Aus seiner Sicht muss auch bei unterschiedlichen Einsatzszenarien ein angemessenes Datenschutzniveau erhalten bleiben.

21.2.9 Radio Frequency Identification RFID

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Es handelt sich dabei um Infomationsträger, die berührungslos per Funk ausgelesen werden können (Transponder). Schon jetzt werden viele Bereiche mit RFID-Lösungen ausgestattet, und es ist zu erwarten, dass künftig neben Lebensmitteln auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. Die RFID-Kennungen der einzelnen Gegenstände können mit personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden und ermöglichen auf diese Weise detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile.

Um dem entgegenzuwirken und den Schutz der Persönlichkeitsrechte Betroffener sicherzustellen, sind folgende Anforderungen von Bedeutung:

- Transparenz
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

- Kennzeichnungspflicht
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

- Deaktivierung
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dies in einer Entschließung zum Ausdruck gebracht (Anlage 16) und verbindliche Regelungen für den Einsatz von RFID-Lösungen gefordert. Sie erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten.

Hierzu hat der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum datenschutzgerechten Einsatz von RFID-Lösungen erstellt (http://www.datenschutz.rlp.de/).

21.2.10 Elektronische Signatur

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. In Form der qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG dient die Elektronische Signatur dem Nachweis der Echtheit elektronischer Dokumente und ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten jedoch einen Trend, in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So wurde beispielsweise beim Verfahren Elster Online der Finanzverwaltung das in § 87a Abs. 3 AO geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Aus Sicht der Datenschutzbeauftragten muss dem entgegengetreten werden. Obwohl Signatur- und Authentisierungsverfahren vergleichbare technische Verfahren nutzen, unterscheiden sie sich jedoch im Inhalt ihrer Aussagen.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Eine in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus können sie Nachteile für die Nutzenden mit sich bringen. Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Forderung an den Gesetzgeber erhoben, keine ungeeigneten Verfahren zuzulassen (Anlage 13). Dies bedeutet, dass den Nutzern die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Signaturverfahren müssen immer dann eingesetzt werden, wenn Aussagen über Dokumente oder Nachrichten gefordert sind, Authentisierungsverfahren dort, wo es um Aussagen über eine Person oder eine Systemkomponente geht.

21.3 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren

21.3.1 Integriertes rheinland-pfälzisches Mittelbewirtschaftungs- und Anordnungsverfahren IRMA

Das FM betreibt seit Jahren das „Integrierte rheinland-pfälzische Mittelbewirtschaftungs- und Anordnungsverfahren“ (IRMA) als dezentrale Lösung zur Verwaltung der Haushaltsmittel in den einzelnen Ressorts. Im Zuge der Weiterentwicklung des Verfahrens hin zu einer webbasierten Anwendung, die durch den LDI zentral für alle Ressorts und teilweise auch nachgeordnete Dienststellen betrieben wird, wurde der LfD bereits während der Entwicklungsphase eingebunden, um datenschutzrelevante Belange in die Verfahrensentwicklung einzubringen. Gegenüber dem bisherigen IRMA-Verfahren konnte eine deutliche Verbesserung der Nachvollziehbarkeit von Verarbeitungsschritten innerhalb des Verfahrens erzielt werden, wobei gleichzeitig die Verarbeitung personenbezogener Informationen reduziert werden konnte.

Regelmäßig wiederkehrende Auswertungen auf den Buchungsdatenbestand konnten standardisiert und so aufbereitet werden, dass möglichst anonymisierte Daten ausgegeben werden. Sofern personenbezogene Daten mit ausgewertet werden, erfolgt eine umfassende Protokollierung, um eine missbräuchliche Nutzung aufklären zu können. Zur Auswertung dieser Protokolldaten wurden eigene Berechtigungsrollen innerhalb des Verfahrens geschaffen, um gleichzeitig den Schutz der Personaldaten gegen unzulässige Leistungskontrolle zu gewährleisten. Die Rolle der Protokollrevision soll gemäß der zum Verfahren erlassenen Musterdienstanweisung regelmäßig beim behördlichen Datenschutzbeauftragten der verantwortlichen Stelle eingerichtet werden.

Freie Auswertungen auf den Buchungsdatenbestand werden innerhalb der Dienststellen nur bei einzelnen Bediensteten zugelassen. Da bei diesen Auswertungen grundsätzlich Teile der Datenbank für eine mögliche Weiterverarbeitung aufbereitet und aus dem Protokollschema des Verfahrens herausgelöst werden können, wird die Anwahl dieser Auswertungen mit Angabe des Abfragegrundes und der genauen Abfrageparametern protokolliert. Sofern die Datenbankextrakte in den Dienststellen durch eigene Verfahren weiterverarbeitet werden, gelten für diese Verfahren die gleichen Rahmenbedingungen wie für das Verfahren WebIRMA, wobei die Verantwortung und die Kontrollpflichten aus § 9 LDSG dann auf die auswertende Stelle übergehen.

Einvernehmlich wurde zwischen dem Ministerium der Finanzen, dem LfD und dem das Verfahren betreuende Softwarehaus vereinbart, dass bei Bedarf weitere „Standardabfragen“ ins Verfahren aufgenommen werden, um „Freie Abfragen“ weiterhin zu reduzieren und die Nachvollziehbarkeit der Verfahrensnutzung stetig zu verbessern. Der LfD wird die Verfahrensnutzung weiterhin begleiten und im kommenden Berichtszeitraum durch örtliche Feststellungen überprüfen.

21.3.2 Elektronische Wirkungsanalyse von Sozialleistungen EWAS

Das Land Rheinland-Pfalz erprobt im Rahmen des Projekts „Elektronische Wirkungsanalyse in der Sozialhilfe (EWAS)“ gemeinsam mit sechs Pilotkommunen eine ziel- und wirkungsorientierte Steuerung von Sozialhilfeleistungen. Anhand sog. „Wirkungsindikatoren“ soll dabei die Effektivität und Effizienz von Sozialhilfeleistungen evaluiert werden. Dies wird unterstützt durch den Einsatz eines automatisierten Verfahrens, welches für die Analyse und Steuerung auf die relevanten Daten aus den Sozialhilfeverfahren der beteiligten Kommunen zurückgreift.

Die im Verfahren EWAS beabsichtigte Wahrnehmung zentraler Aufgaben durch das LSJV kann aus Sicht des LfD grundsätzlich im Wege der Auftragsdatenverarbeitung erfolgen. Voraussetzung ist aus seiner Sicht jedoch, dass entsprechende Verwaltungsvereinbarungen getroffen werden und eine klare Zuordnung der Verantwortlichkeiten zwischen den beteiligten Stellen vorgenommen wird.

Das zum Verfahren erstellte Datenschutzkonzept sieht vor, dass die Auswertung grundsätzlich anhand pseudonymisierter Daten erfolgt. Die Pseudonymitätsbildung erfolgt dabei nach einem einheitlichen Verfahren. Überlegungen des LfD, eine kommunenindividuelle Verschlüsselung einzusetzen, konnte mit Blick auf häufige Wanderungsbewegungen, die zu notwendigen Zugriffen auch durch andere als die ursprünglich verschlüsselnde Kommune führen, nicht entsprochen werden. Daraus ergab sich, dass die für EWAS erhobenen Daten in einem einheitlich verschlüsselten, pseudonymen zentralen Datenbestand vorgehalten werden. Aus Sicht des LfD bedurfte es hierbei geeigneter Vorkehrungen, die missbräuchliche Zugriffe verlässlich ausschließen.

Hierzu zählte neben einem entsprechenden Berechtigungskonzept eine Verfahrensweise, die Probeangriffe, durch die Bildung eines Pseudonyms für eine Person anhand der relevanten Angaben (Name, Vorname, Geburtstag, Geburtsort) mit dem Ziel festzustellen, ob ein solches bereits vorhanden ist, wirksam verhindert. Dem wurde entsprochen, indem bei der Pseudonymisierung eine ergänzende Information eingeht (Zufallszahl), durch die ein Probeangriff bzw. der Versuch einer Reidentifizierung außerhalb dieses „Treuhändermoduls“ ausgeschlossen wird. Den insoweit ergangenen Vorschlägen des LfD wurde entsprochen. Im Rahmen des Pilotbetriebes wird der LfD deren Umsetzung kontrollieren.

21.3.3 Aufbau eines Verordnungsinformationssystems der Kassenärtzlichen Vereinigung Rheinland-Pfalz

Um Informationen über die Verordnungsentwicklung zu erhalten und den niedergelassenen Ärzten in Rheinland-Pfalz einen zeitnahen Überblick über die vorgenommenen Verordnungen zu ermöglichen, hat die KV Rheinland-Pfalz ein entsprechendes Verordnungsinformationssystem (VIS) entwickelt. Mit Blick auf die datenschutzrechtliche Notwendigkeit, einen Versichertenbezug der Analysen zu vermeiden, wurde der LfD Rheinland-Pfalz um Beratung gebeten.

Problematisch war in diesem Zusammenhang anfangs die vorgesehene Zusammenführung der über die Apothekenrechenzentren bereitgestellten Verordnungsdaten und der Abrechnungsdaten der KV anhand der Versicherungsnummer. Ein vom LfD für die Pseudonymisierung und zum Schutz vor Probeverschlüsselungsangriffen zunächst ins Auge gefasster Austausch der Versichertennummer durch einen Hashwert plus Zufallszahl schied aufgrund des quartalsübergreifend benötigten Fallzusammenhangs aus. In Zusammenarbeit mit der KV wurde daraufhin ein Konzept abgestimmt, das in Anlehnung an die Verfahrensweise des Krebsregisters Rheinland-Pfalz bzw. der Datenstelle für Disease-Management-Programme der KV Rheinland-Pfalz eine Vertrauensstelle für die Zusammenführung der Datenbestände vorsieht. Dieser wird über entsprechende Regelungen für die Wahrnehmung ihrer Aufgaben die erforderliche interne Unabhängigkeit eingeräumt. Diese Regelungen sehen u.a. die organisatorische, personelle und technische Trennung zwischen Pseudonymisierung und Betrieb und Nutzung des Arzneimittelinformationssystems vor.

Die Verordnungsdaten werden von den liefernden Apothekenrechenzentren mit verschlüsselter Versicherungsnummer zur Verfügung gestellt, so dass der Patientenbezug für die KV nicht mehr erkennbar ist. Die benötigten Daten werden auf einem Webserver zum Abruf bereitgestellt. Der Zugang zum Webserver erfolgt via Internet. Über das HTTPS-Protokoll wird dabei ein sicherer Übertragungskanal aufgebaut (SSL/TLS 128 Bit). Als in bestimmten Szenarien notwendige Alternativlösung erfolgt der Versand der Daten per E-Mail; in diesem Fall wird der gesamte Datenbestand zusätzlich transportverschlüsselt. Von der „Vertrauensstelle“ der KV werden die empfangenen Verordnungsdaten in das Arzneimittelinformationssystem übernommen; die Transferdatei wird nach erfolgreicher Übernahme gelöscht. Die notwendigen Arbeitsschritte werden dabei in einem weitgehend automatisierten Prozess abgebildet, der kein manuelles Eingreifen erfordert. Für die bei der KV bereits vorhandenen

Abrechnungsdaten der korrespondierenden Quartale werden durch die „Vertrauensstelle“ die Versichertennummern pseudonymisiert und die Daten ebenfalls in das Arzneimittelinformationssystem übernommen.

Die Software für die Verschlüsselung der Versichertennummern wird dabei von der „Vertrauensstelle“ der KV entwickelt und den datenliefernden Stellen zur Verfügung gestellt. Der verwendete Schlüssel ist fest und vor unbefugtem Auslesen geschützt in das Programm eingebunden. Eine Sicherungskopie des Schlüssels und des Programmquellcodes ist bei einer dritten Stelle gegenüber unbefugtem Zugriff geschützt hinterlegt. Eine darüber hinausgehende Speicherung des Schlüssels erfolgt nicht. Für den Fall der Kompromittierung des Schlüssels oder eines notwendigen Wechsels des Algorithmus wurde ein Verfahren festgelegt, das bei Bedarf einen Umstieg ermöglicht.

Im Ergebnis stellt das Verfahren in angemessener Weise sicher, dass die Kenntnis des Schlüssels und die Kontrolle über das Verschlüsselungsprogramm ausschließlich bei der Vertrauensstelle liegen, und die das Arzneimittelinformationssystem nutzenden Stellen der KV keine Zuordnung eines Pseudonyms zur zugehörigen Versichertennummer vornehmen können.

21.3.4 Elektronischer Reisepass (ePass) und Personalausweis (ePA)

Mit einer Verordnung des Europäischen Rates aus dem Jahr 2004 wurden die Mitgliedstaaten unter Vorgabe von Fristen verpflichtet, in die Reisepässe einen RFID-Chip zu integrieren. Auf diesem Chip sollen neben den bisherigen Passdaten einschließlich eines Gesichtsbildes auch Fingerabdrücke gespeichert werden. Mit der Ausgabe sog. ePässe, die als elektronisch lesbares biometrisches Merkmal ein Gesichtsbild enthalten, wurde bereits begonnen. Ab dem 1.11.2007 werden zusätzlich zwei Fingerabdrücke (rechter und linker Zeigefinger) in den biometriegestützten ePass aufgenommen – ePässe der zweiten Generation. Über die europarechtlichen Regelungen hinaus plant die Bundesregierung Maßnahmen, um dies auch beim Personalausweis einzuführen.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder auf die aus ihrer Sicht ungenügende Sicherung der biometrischen Daten vor einem unbemerkten Auslesen durch unbefugte Dritte hingewiesen und vor einer übereilten Einführung der biometrischen Pässe gewarnt. Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung aus dem Jahr 2005 u.a. Folgendes gefordert:

Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird, dass

- die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Die hinsichtlich der Einführung biometrischer Merkmale in den Reisepass geäußerten Bedenken erhalten beim Personalausweis dadurch noch eine andere Dimension, dass die meisten Erwachsenen ihren Personalausweis – im Gegensatz zum Reisepass – ständig bei sich tragen.

Mit den ePässen der zweiten Generation wird nunmehr der erweiterte Zugriffsschutz – Extended Access Control (EAC) – eingeführt. Damit soll zum einen gewährleistet werden, dass nur berechtigte, hoheitliche Lesegeräte auf die im RFID-Chip gespeicherten Fingerabdrücke zugreifen können. Zum anderen soll auch der Schutz aller personenbezogenen Daten entsprechend den Hinweisen des BSI erhöht werden. Nicht unproblematisch ist allerdings, dass sich Falscherkennungen durch die Einführung der Fingerabdrücke noch verstärken können. Schätzungen zufolge besitzen etwa 2 % der Bevölkerung keine aussagekräftigen Fingerabdrücke oder die Fingerabdrücke verändern sich nach Passausstellung z.B. durch bestimmte körperliche Arbeiten.

Zur Einführung der ePässe der zweiten Generation sah § 23a PassG ein Testverfahren vor. Von technisch entsprechend ausgestatteten Behörden wurden testweise im Rahmen des Antragsverfahrens zur Ausstellung eines ePasses erster Generation

Fingerabdrücke an die Bundesdruckerei übermittelt. Die Passbewerber nahmen auf freiwilliger Basis an dem Test teil. Die per Fingerabdruckscanner aufgenommenen Daten wurden nicht in dem beantragten ePass erster Generation gespeichert.

Die Datenschutzbeauftragten des Bundes und der Länder werden die weitere Entwicklung intensiv beobachten.

21.3.5 Prüfungsanmeldung via Internet

Aus dem Bereich der Hochschulen wurde der LfD in mehreren Fällen wegen der Gestaltung von Onlineverfahren für die Anmeldung zu Prüfungen über das Internet angesprochen. Aus Sicht des LfD hat sich hierfür sowie für vergleichbare Szenarien eine zweistufige Verfahrensweise als geeignet erwiesen. Dabei wird zunächst die Einrichtung eines Zugangs bzw. die Vergabe einer Benutzerkennung per Webformular über eine geschützte Verbindung (HTTPS-Protokoll) beantragt. Zum Nachweis der Identität der Antragsteller werden dabei bestimmte, von der Universität überprüfbare Angaben sowie eine gültige E-Mail-Adresse erfragt. Dabei sollte es sich um solche Angaben handeln, die nur dem Betroffenen und Dritten nicht ohne Weiteres bekannt sind (z.B. Immatrikulationsnummer, Name, Vorname, Geburtsdatum und Geburtsort). Im zweiten Schritt wird ein individuelles Einmalpasswort erzeugt und an die angegebene E-Mail-Adresse übermittelt. Dieses ermöglicht die erstmalige Anmeldung im Verfahren. Im Anschluss daran werden die Studierenden aufgefordert, ein eigenes Passwort zu vergeben. Dabei verbleibt gleichwohl das Restrisiko eines unbefugten Zugangs, etwa wenn die erfragten Daten Dritten bekannt sind bzw. erraten werden können. Daher sollte nach Möglichkeit eine E-Mail-Adresse verwendet werden, die bei der jeweiligen Einrichtung bereits hinterlegt ist.

Für Lösungen, die die Betroffenen freiwillig in Anspruch nehmen können, ist dieses Verfahren aus Sicht des LfD datenschutzrechtlich akzeptabel. Soweit die Art der betroffenen Daten es gebietet oder eine zusätzliche Absicherung erforderlich ist, sollte die Anmeldung an zusätzliche Mechanismen gebunden werden, die eine hinreichend verlässliche Authentifizierung der Nutzer erlaubt, etwa eine Studierendenkarte oder Verfahren der elektronischen Signatur.

21.3.6 Datensicherheit beim Betrieb einer Internetpräsenz für Onlineumfragen

Im Rahmen der Durchführung einer wissenschaftlichen Studie an einer rheinland-pfälzischen Schule war vorgesehen, die für die Datenerhebung verwendeten Fragebögen sowohl auf Papier als auch als Onlineversion im Internet anzubieten. Nach den Planungen der verantwortlichen Stelle sollte für Letzteres auf ein entsprechendes Angebot einer in der Schweiz ansässigen Firma zurückgegriffen werden.

Für das unter der entsprechenden Internet-Adresse erreichbare System hat sich bei einer Sichtung ergeben, dass auch außerhalb der den Kunden angebotenen Onlineformulare Zugriffe auf Benutzerdaten möglich waren. So konnten, ohne besondere Sicherungen überwinden zu müssen, kundenspezifische Daten und Dokumente anderer Nutzer sowie Protokolldateien mit aufgezeichneten Zugriffen auf die Inhalte der o.g. Internetpräsenz eingesehen werden.

Aufgrund der sich daraus ergebenden Zweifel, ob der Betrieb der Seite den Anforderungen des rheinland-pfälzischen Datenschutzgesetzes an eine angemessene Zugriffskontrolle entspricht, hat der LfD empfohlen, von dieser Möglichkeit der Onlineumfrage für die Studie zunächst abzusehen und den Datenschutzbeauftragten des Kantons Bern als zuständige Aufsichtsbehörde unterrichtet.

21.3.7 Verfahren DMP-Online der Datenstelle Disease-Management-Programme

Über die Strukturen zur Durchführung von Disease-Management-Programmen hat der LfD bereits im 19. Tb., Tz. 11.5 sowie im 20. Tb., Tz. 11.2 berichtet. In Fortentwicklung des bei der Kassenärztlichen Vereinigung Rheinland-Pfalz eingesetzten Verfahrens wurde eine Möglichkeit vorgesehen, die DMP-Daten online zur Verfügung zu stellen.

Den im Rahmen seiner Beratung vom LfD gegebenen Hinweisen für eine angemessene Zugangs-, Zugriffs- und Weitergabekontrolle i.S. der Anlage zu § 78 a Nr. 2 bis 4 SGB X wurde entsprochen. So sieht das Verfahren den Einsatz eines Virtuellen Privaten Netzes vor, welches eine vertrauliche Übermittlung der DMP-Daten ermöglicht und in Verbindung mit dem Einsatz von Zertifikaten auf Client- und Serverseite eine verlässliche Authentifizierung der Teilnehmer gewährleistet.

Das Konzept sah weiterhin vor, dass die Serversysteme durch einen Dienstleister betrieben werden können. Eine solche Auftragsdatenverarbeitung wird durch § 80 SGB X grundsätzlich ermöglicht, ist jedoch im Fall der Beauftragung einer nicht-öffentlichen Stelle an die besonderen Voraussetzungen des § 80 Abs. 5 SGB X gebunden. Danach ist sie nur zulässig, wenn beim Auftraggeber ansonsten Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten erheblich kostengünstiger

besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes umfasst. Für die Zulässigkeit einer Auftragsverarbeitung kam es mithin darauf an, dass der überwiegende Teil des Datenbestandes in der Hand der Datenstelle Trier verblieb. Der Betrieb eines zentralen elektronischen Archivs durch einen nicht-öffentlichen Auftragnehmer schied damit in der vorgesehenen Form aus. Die Annahme der elektronisch angelieferten DMP-Daten und deren Zwischenspeicherung bis zur Weiterleitung an die Datenstelle Trier konnten hingegen grundsätzlich im Wege der Auftragsdatenverarbeitung erfolgen. Die Datenstelle bleibt in diesem Fall nach § 80 Abs. 1 SGB X weiterhin die datenschutzrechtlich verantwortliche Stelle.

Da die DMP-Daten dem Arztgeheimnis nach § 203 Abs. 1 Nr. 1 StGB unterliegen, muss in Verbindung mit § 80 Abs. 1 SGB X auch im Fall der Datenverarbeitung im Auftrag sichergestellt werden, dass eine unbefugte Offenbarung der Patientendaten ausgeschlossen wird. Die hierzu vorgesehene Verschlüsselung innerhalb der Datenbank des DMP-Onlineverfahrens war aus Sicht des LfD geeignet. Um eine § 203 StGB vergleichbare Strafbarkeit zu gewährleisten, hat der LfD empfohlen, eine Verpflichtung der betroffenen Mitarbeiter des Auftragnehmers nach dem Verpflichtungsgesetz vorzunehmen.

Die Sicherheit eines solchen Verfahrens hängt letztlich von der Sicherheit aller beteiligten Stellen und Komponenten ab. Für die Übertragung der DMP-Daten ist dies mit den o.g. Mechanismen und für die Datenstelle mit deren IT-Strukturen und organisatorischen Abläufen gewährleistet. Für den Bereich der Arztpraxen muss dies jedoch in gleicher Weise gelten. Die Übermittlung der DMP-Daten erfolgt über das Internet und erfordert somit einen entsprechenden Zugang der Arztsysteme. Daraus ergibt sich die Notwendigkeit, diese gegenüber unbefugten Zugriffsversuchen aus dem Internet und den Risiken etwaiger Schadenssoftware abzusichern. Die Situation in den Arztpraxen ist nach Einschätzung des LfD in diesem Punkt durchaus unterschiedlich zu bewerten. Nach seiner Kenntnis greift zwar ein Teil der Ärzteschaft auf Provider zurück, die speziell gesicherte Internetzugänge anbieten; aus Sicht des LfD kann dies jedoch nicht allgemein vorausgesetzt werden. Eine unzureichend geschützte Internetanbindung des Systems, über welches die DMP-Daten versendet werden, entspräche nicht den Vorgaben des § 78a SGB X. Bei den teilnehmenden Praxen muss daher gewährleistet sein, dass diese über geeignete technische Vorkehrungen verfügen. Mit Blick auf die datenschutzrechtliche Zuständigkeit der Aufsichts- und Dienstleistungsdirektion Trier in diesem Bereich hat der LfD diese über das Verfahren unterrichtet.

22. Öffentlich-rechtliche Wettbewerbsunternehmen

22.1 Was geht den zukünftigen Vermieter die Religionszugehörigkeit an?

Wie alle Vermieter möchten auch kommunale Wohnungsbaugesellschaften als öffentlich-rechtliche Wettbewerbsunternehmen vermeiden, dass Mietnomaden bei ihnen einziehen. Zudem legen sie bei der Mieterzusammensetzung Wert darauf, dass keine sozialen Brennpunkte entstehen. Dabei spielt in der Regel auch die Religion der Mieter eine wesentliche Rolle.

Grundsätzlich dürfen auch bereits vor Abschluss des Mietvertrages geeignete Daten auf freiwilliger Basis erhoben werden. Für Vermieter waren insbesondere folgende Punkte von Interesse:

Fragen nach Gehalt und Arbeitgeber seien besonders wichtig zum Schutz vor Mietnomaden. Eine gesetzliche Verpflichtung zur Angabe besteht nicht. Bei Hinweis auf die Freiwilligkeit der Angaben kann aus Sicht des LfD hiernach aber gefragt werden. Wenn ein Mietbewerber sich jedoch weigert, die Angaben zu machen, kann er hierzu nicht gezwungen werden.

Die Verwendung des Personalausweises im nichtöffentlichen Bereich ist in § 4 des PAuswG geregelt. Danach kann der Personalausweis auch im nichtöffentlichen Bereich als Ausweislegitimationspapier benutzt werden. Die Seriennummern dürfen nicht so verwendet werden, dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Der Personalausweis darf weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung solcher Daten verwendet werden. Soweit diese Vorgaben eingehalten werden, bestehen keine datenschutzrechtlichen Bedenken, sich den Personalausweis bei der Bewerbung um eine Wohnung vorlegen zu lassen.

Kopien von Gehaltsbescheinigungen oder Personalausweisen sollten nur dann zur Akte genommen werden, wenn der Bewerber zuvor auf die Freiwilligkeit hingewiesen wurde und er der Maßnahme zugestimmt hat. Ansonsten sollten Vermieter sich darauf beschränken, die durch Vorlage der genannten Dokumente erworbenen Erkenntnisse anderweitig festzuhalten.

Fragen nach der Religionszugehörigkeit hält der LfD für unzulässig. Die Religionsfreiheit ist durch das Grundgesetz garantiert. Hiervon ist auch die Preisgabe der eigenen religiösen Überzeugung umfasst. Eine Einschränkung dieses Grundrechts ist nur aufgrund eines Gesetzes zulässig. Nur auf Grundlage eines solchen Gesetzes dürfte ausnahmsweise nach der Religionszugehörigkeit gefragt werden. Eine entsprechende Rechtsnorm besteht hier aber nicht.

Das Erheben der Staatsangehörigkeit ist nur aufgrund einer gesonderten Einwilligung der Betroffenen zulässig. Hierbei handelt es sich um eine besondere Art personenbezogener Daten gem. § 3 Abs. 9 BDSG. Diese Daten stehen unter dem ausdrücklichen Schutz der Rechtsordnung. Daher sind besondere Anforderungen an die Einwilligung gem. § 4a Abs. 3 BDSG zu stellen.

22.2 Glücksspielstaatsvertrag

Im nächsten Jahr soll ein neuer Glücksspielstaatsvertrag in Kraft treten. Darin ist eine Spielersperre vorgesehen, die in einer Sperrdatei einzutragen ist. Es wird zwar geregelt, welche Daten wie lange in der Sperrdatei verarbeitet werden dürfen, es ist jedoch nicht ersichtlich, wo diese Sperrdatei geführt werden soll. Von einigen Spielbanken des Landes Rheinland-Pfalz wurde die Frage an den LfD herangetragen, wie sie mit den bereits vorhandenen Daten über Spielersperren zu verfahren haben. Dabei ist insbesondere von Interesse, ob sie diese Daten an andere zur Teilnahme am Sperrsystem verpflichteten Veranstalter übermitteln dürfen. Der LfD ist derzeit um Klärung bemüht, wie eine solche Spielerdatei ausgestaltet werden soll, um die datenschutzrechtlichen Aspekte prüfen zu können. Da die Zuständigkeit für die Spielbanken des Landes bei der Aufsichts- und Dienstleistungsdirektion liegt, wurde diese ebenfalls beteiligt.

22.3 Die „SWIFT"-Affäre – Zweiter Teil

Bereits an anderer Stelle unter Tz. 2.7 wurde dargestellt, dass sowohl der Düsseldorfer Kreis als auch die Artikel 29-Gruppe in dem o.g. Zusammenhang festgestellt haben, dass Vorgaben der EG-Datenschutzrichtlinie durch SWIFT bzw. der sich der Dienstleistungen von SWIFT bedienenden Finanzinstitute nicht beachtet wurden. U.a. wurde als sofortige Maßnahme zur Verbesserung der derzeitigen Situation gefordert, dass alle Finanzinstitute ihre Kunden angemessen über die Tatsache informieren, dass die Datensätze auch an ein in den USA ansässiges SWIFT Rechenzentrum übermittelt werden, wodurch die US-Behörden Zugriff auf die Daten haben.

Der LfD, dessen Zuständigkeit auf die öffentlich-rechtlichen Kreditinstitute beschränkt ist, hatte sich daraufhin an die Landesbank Rheinland-Pfalz sowie an den Sparkassen- und Giroverband Rheinland-Pfalz mit der Bitte gewandt, zu den insoweit ergriffenen Maßnahmen zu berichten. Der Sparkassen- und Giroverband hatte ein vom Zentralen Kreditausschuss entwickeltes Kundeninformationsblatt bereits im Dezember 2006 allen rheinland-pfälzischen Sparkassen zur Verfügung gestellt. Gleichzeitig hat der Sparkassen- und Giroverband in seiner Stellungnahme angemerkt, dass ein deutsches Kreditinstitut ohne Zusammenarbeit mit SWIFT seinen Kunden keine Dienstleistungen im weltweiten Zahlungsverkehr anbieten könnte. Die Landesbank Rheinland-Pfalz hat im Januar 2007 nachgezogen und eine Kundeninformation online zur Verfügung gestellt.

23. Sonstiges

23.1 Videoüberwachungen in Rheinland-Pfalz

Journalisten haben wiederholt gefragt, ob und in welchem Umfang „Straßen und Plätze" in Rheinland-Pfalz derzeit überwacht werden. Der LfD hat diese Anfragen stets wie folgt beantwortet:

Nach seiner Kenntnis würden in Rheinland-Pfalz durch Polizei- bzw. Ordnungsbehörden des Landes dauerhaft weder Straßen noch Plätze von Videokameras erfasst. Eine Rechtsgrundlage hierfür könnte sich ggf. in § 27 POG finden (s.Tz. 18.2). Anlassbezogen (d.h. bei Fußballspielen) werde in Kaiserslautern der Zuweg zum Fußballstadion mit – zwar dauerhaft installierten, aber nur zeitweise genutzten – Videokameras auf der Grundlage des § 27 POG überwacht. Wesentlich zu unterscheiden von diesem Bereich ist die Sicherung von Gebäuden auch im Bereich der äußeren Zugänge (z.B. Rathäuser, öffentliche Bibliotheken, aber auch Justizvollzugsanstalten) und bestimmten Liegenschaften (beispielsweise Friedhöfe, Schwimmbäder) durch die Stellen, die Inhaber des Hausrechts sind und die u.a. auch die Verhinderung von Vandalismusschäden zum Ziel haben. Eine Rechtsgrundlage hierfür besteht in Bezug auf öffentliche Stellen des Landes in § 34 LDSG. Eine flächendeckende Übersicht über die tatsächliche Nutzung der Videotechnik durch öffentliche Stellen in diesem Zusammenhang hat der LfD nicht; häufig wird er allerdings hier um Rat gefragt, unter welchen rechtlichen und tatsächlichen Voraussetzungen diese Technik eingesetzt werden darf. Soweit private Hausrechtsinhaber auf der Grundlage von § 6 b BDSG tätig werden, ist für den privaten Bereich in Rheinland-Pfalz die ADD zuständige Datenschutzaufsichtsbehörde. Weiter ist von diesen Maßnahmen zu unterscheiden der Einsatz von Webcams durch Gemeinden, die insbesondere das Ziel der Tourismuswerbung verfolgen. Nicht selten werden zentrale Plätze von Gemeinden aufgenommen; bei häufigen (etwa minütlichen) Bilderneuerungen und bei Nahaufnahmen der Kamera kann hier die Grenze zu einer (unzulässigen) „Überwachung" überschritten werden. In Rheinland-Pfalz hat der LfD versucht, dem durch allgemeine Vorgaben entgegen zu treten (s. Tz. 18.1). In diesem Zusammenhang können auch die Webcams erwähnt werden(s. Tz. 14.2), die durch den Landesbetrieb Mobilität (den ehemaligen Landesbetrieb Straßen

und Verkehr) insbesondere auf bestimmten Autobahnabschnitten an Baustellen eine Übersicht über die Verkehrsbelastung erlauben (vgl. http://www.lbm.rlp.de/Frames/index.asp?bereich=105).

Nicht der Zuständigkeit des LfD unterliegt die Frage, inwieweit durch die Bahn AG bzw. die Bundespolizei beispielsweise auch die Umgebung von Bahnhöfen von Videokameras erfasst wird. Darüber hat er keine konkreten Erkenntnisse. Insoweit ist für die Bahn AG der Berliner Beauftragte für Datenschutz und Informationsfreiheit, für die Bundespolizei der BfDI zuständig.

23.2 Unzulässige Übermittlung eines Beschwerdeschriftwechsels

Eine Petentin hatte die ihr von ihrem Arbeitgeber zur Verfügung gestellte E-Mail-Adresse während der üblichen Arbeitszeiten dazu genutzt, über einen längeren Zeitraum hinweg zahlreiche Beschwerden zur Vorgehensweise einer bundesweit tätigen Institution über einen breiten Verteiler an namhafte Vertreter des öffentlichen Lebens zu versenden. Die unter den Bundesländern federführend für die Zusammenarbeit mit dieser Institution zuständige öffentliche Stelle des Landes Rheinland-Pfalz hatte sich im Rahmen eines längeren Schriftwechsels – aus dortiger Sicht erfolglos – um einen konstruktiven Dialog mit der Petentin bemüht. Dabei war die öffentliche Stelle davon ausgegangen, dass die Petentin aus ihrer beruflichen Aufgabenstellung heraus agierte. Nachdem die Petentin dann auch für die fragliche Institution ehrenamtlich tätige Personen u.a. mit pauschalen und persönlichen Unterstellungen sowie unsachlichen Äußerungen angegangen habe, habe man sich dazu entschieden, den Arbeitgeber der Petentin zur weiteren Klärung über den Sachverhalt zu informieren. Die öffentliche Stelle sah sich hierzu aufgrund einer gegenüber den ehrenamtlich tätigen Personen bestehenden Fürsorgepflicht veranlasst und gleichzeitig berechtigt.

Die Petentin machte dagegen geltend, dass sie sich als Privatperson an die öffentliche Stelle gewandt habe und deshalb mit der teilweisen Weiterleitung des geführten Schriftwechsels an ihren Arbeitgeber nicht einverstanden sei. Sie fühle sich durch diese Vorgehensweise gegenüber ihrem Arbeitgeber denunziert.

Der LfD hat gegenüber der öffentlichen Stelle die Auffassung vertreten, dass die von der Petentin beanstandete Datenübermittlung an ihren Arbeitgeber nicht hinnehmbar ist, da sie nicht als erforderliche Reaktion auf die Beschwerden der Petentin im Zusammenhang mit der dargestellten Fürsorgepflicht gegenüber der ehrenamtlich tätigen Fachkräften angesehen werden kann. Für den LfD haben sich nach intensiver Prüfung der vorgelegten Unterlagen keine durchgreifenden Anhaltspunkte dafür ergeben, dass die öffentliche Stelle von der Annahme überzeugt sein durfte, dass die Petentin die Beschwerde-E-Mails im Rahmen ihrer beruflichen Aufgabenstellung verfasst hat. Nur in einem solchen Fall hätte man sich mit dem Arbeitgeber der Petentin in Verbindung setzen dürfen, ohne insoweit bei der Petentin vorher nachzufragen. Zwar hatte die Petentin für die Versendung ihrer Schreiben die dienstliche E-Mail-Adresse während der üblichen Arbeitszeiten verwendet. Gegen eine begründete Annahme, dass die Petentin im Rahmen ihrer beruflichen Aufgabenstellung tätig geworden ist, sprachen aber Anmerkungen im Schriftwechsel, dass sie die darin geäußerten Ansichten „als Mutter“ vertritt. Insgesamt ging es der Petentin vielmehr darum, die bei der oben genannten Institution tätigen Fachkräfte von ihrer eigenen, privaten Meinung zu deren Entscheidungen zu überzeugen.

Die Datenübermittlung an den Arbeitgeber der Petentin war somit aus datenschutzrechtlicher Sicht ohne Rechtsgrundlage erfolgt. Da sich die fragliche Stelle der Rechtsauffassung des LfD angeschlossen hat, konnte von einer förmlichen Beanstandung abgesehen werden.

24. Öffentlichkeitsarbeit

24.1 Ausstellung zum Europäischen Datenschutztag 2007

Der Europarat hat mit verschiedenen Aktionen am 29.1.2007, dem ersten Europäischen Datenschutztag, versucht, die Menschen europaweit für ihre Datenschutzrechte zu sensibilisieren. Ziel war, das Bewusstsein für den Datenschutz bei den Bürgern in Europa erhöhen. Die mit dem Datenschutz befassten Stellen in Europa haben sich mit eigenen Aktionen an diesem Tag beteiligt. Er soll zukünftig jährlich regelmäßig in der Woche um den 28. Januar terminiert werden, weil an diesem Datum die Unterzeichnung der Europaratskonvention 108 zum Datenschutz begonnen wurde. Mit der Konvention verpflichten sich die unterzeichnenden Staaten, für die Achtung der Rechte und Grundfreiheiten insbesondere des Persönlichkeitsbereichs bei der automatisierten Datenverarbeitung Sorge zu tragen.

Der rheinland-pfälzische Datenschutzbeauftragte hat die Initiative für einen Datenschutztag begrüßt und unterstützt, weil sie einen Anlass gibt, in einer Zeit, in der Datenverarbeitung allgegenwärtig ist, die im Interesse des Schutzes von Privatsphäre

bestehenden Regelungen darzustellen, auf die Gefahren hinzuweisen sowie den Bürgerinnen und Bürgern Möglichkeiten zum „Selbstdatenschutz“ nahezubringen. Er hat anlässlich dieses Tages eine Ausstellung gestaltet, die die Entwicklung der Datenverarbeitung und des Datenschutzes, aktuelle Probleme dieser Bereiche und die Mechanismen zum Schutz der Persönlichkeitsrechte der Menschen in diesem Zusammenhang darstellt. Ihr Titel lautet „Aus!geschnüffelt?, Entwicklung und aktuelle Probleme des Datenschutzes“. Sie wurde in Mainz mit einem Vortrag vom Vizepräsidenten des Bundesverfassungsgerichts, Universitätsprofessor Dr. Winfried Hassemer, eröffnet. In einer Begleitbroschüre ist der Inhalt der Ausstellung veröffentlicht worden. Parallel hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine zentrale Diskussionsveranstaltung in Berlin mit dem Thema „Wie schützt der Staat die Freiheit?“ durchgeführt.

Der LfD ist daran interessiert, seine Ausstellung im Lande möglichst vielen Bürgern zu präsentieren. Dazu bemüht er sich um Kooperationspartner. Dies ist ihm dankenswerter Weise durch das Engagement verschiedener Abgeordneter des Landtags und dank der Unterstützung durch das Innenministerium gelungen.

24.2 Internetauftritt

Nach wie vor stellt die Website des LfD eine wesentliche Komponente seiner Darstellung nach außen dar. Die steigenden Zugriffszahlen belegen, dass dieses Angebot auch von den Bürgern wahrgenommen wird. Allerdings ist eine solche Plattform auch immer verbesserungsbedürftig und -fähig. So hat der LfD es bereits mit Bordmitteln unternommen, die Präsentation seiner aktuellen Hinweise und Presseerklärungen zu verbessern. Er hat eine längere Liste von Wünschenswertem entwickelt, die von verbesserten Suchfunktionen im Angebot über viele weitere Detailänderungen bis zur Entwicklung einer Rubrik „FAQ“ (Frequently Asked Questions, Häufig gestellten Fragen) reicht. Ob dies mit den zur Verfügung stehenden bescheidenen Mitteln erreicht werden kann, muss abgewartet werden.

Darüber hinaus beteiligt sich der LfD nach wie vor auch finanziell am Datenschutzportal der deutschen Datenschutzbeauftragten, dem „Virtuellen Datenschutzbüro“ (http://www.datenschutz.de/).

24.3 Wissenschaftspreis des LfD Rheinland-Pfalz

Für hervorragende wissenschaftliche Arbeiten zum Datenschutz wird der LfD mit Unterstützung des Ministeriums für Bildung, Wissenschaft, Jugend und Kultur im Jahr 2008 erstmals einen Wissenschaftspreis verleihen. Mit dem Preis soll die Bedeutung des in der Landesverfassung ausdrücklich geregelten Rechts auf informationelle Selbstbestimmung und der besondere Stellenwert, den der Datenschutz in Rheinland-Pfalz genießt, unterstrichen werden.

Der Wissenschaftspreis wird in den beiden Kategorien Geistes- und Naturwissenschaften und für besonders qualifizierte Abschlussarbeiten vergeben, die an rheinland-pfälzischen Hochschulen und Forschungseinrichtungen erstellt worden sind. Für interdisziplinäre Arbeiten oder herausragende Arbeiten, die keiner der beiden Kategorien zuzuordnen sind, kann fallweise ein Sonderpreis vergeben werden. Die Dotierung beträgt pro Kategorie jeweils 1.000 Euro. Bewertungskriterien für die Vergabe des Preises sind der Datenschutzbezug, die wissenschaftliche Qualität, der Anwendungsnutzen und der Innovationsgehalt der Arbeit. Der Wissenschaftspreis wird jährlich im Dezember ausgeschrieben und im September/Oktober des folgenden Jahres im Rahmen einer Veranstaltung im rheinland-pfälzischen Landtag verliehen. Bei der Vergabe des Preises wird der LfD durch einen Beirat unterstützt. Diesem gehören je ein Mitglied der im Landtag vertretenen Fraktionen, Vertreter der Landesregierung und der rheinland-pfälzischen Hochschulen sowie Persönlichkeiten aus nichtstaatlichen Bereichen an. Der Beirat befindet über die Vergaberichtlinien und stellt die Mitglieder der für die Auswahl und Bewertung der eingereichten Arbeiten verantwortlichen Jury. Der Beirat soll darüber hinaus datenschutzrechtliche Themenstellungen für die wissenschaftliche Bearbeitung anregen. In diesem Zusammenhang soll er dem LfD auch als Gesprächskreis für aktuelle datenschutzrechtliche Entwicklungen dienen. Angesichts der zunehmenden Durchdringung vieler Lebensbereiche mit Informationstechnik ist es das mit dem Preis verbundene Anliegen des LfD, die wissenschaftliche Behandlung datenschutzrechtlicher Fragen zu fördern und die Entwicklung datenschutzfreundlicher Konzepte zu würdigen, um eine zeitgemäße Umsetzung des Datenschutzes zu unterstützen.

Die Ausschreibung für den Wissenschaftspreis 2008 wird im Dezember 2007 erfolgen. Geeignete Arbeiten können bis zum 30.4.2008 eingereicht werden. Informationen zum Wissenschaftspreis, über die Vergabe und die Möglichkeiten der Bewerbung sind unter http://www.datenschutz.rlp.de/wissenschaftspreis/ abrufbar.

25. Ausblick

Die gegenwärtige Situation des Datenschutzes wird nicht einheitlich beurteilt. Während der Nestor des deutschen Datenschutzes und frühere hessische Landesdatenschutzbeauftragte, Prof. Simitis, in einer aktuellen Veröffentlichung vom „Niedergang des Datenschutzes“ spricht, ist in einem der jüngsten Leitartikel von Heribert Prantl in der Süddeutschen Zeitung vom „Wiederaufstieg des Datenschutzes“ die Rede. Wahrscheinlich stimmt beides, je nachdem, auf welche Aspekte des Datenschutzes der Blick gerichtet wird.

Insoweit ähnelt die Lage des Datenschutzes der sonstiger staatlicher und gesellschaftlicher Daueraufgaben. In angelsächsischen Ländern verwendet man hierfür die Umschreibung „road under construction“. Diese Bezeichnung ist auch für den Datenschutz zutreffend. Auch er gleicht einer im Bau befindlichen Straße: Mancher Streckenabschnitt ist bereits befahrbar, andere sind noch im Bau, wiederum andere vielleicht noch in der Planung, und selbst jene fertigen Teile bedürfen stets der Pflege und Instandhaltung. Mit anderen Worten: Eine solche Straße ist eigentlich niemals fertiggestellt. Das gilt – bildlich gesprochen – für die Demokratie ebenso wie für den Rechtsstaat; es gilt aber eben auch für den Datenschutz im Lande.

Was bedeutet dies konkret? In den beiden vergangenen Jahren hat sich der seit einiger Zeit zu beobachtende Trend fortgesetzt, dass die Kommunikation zunehmend auf der Basis von Techniken des „World Wide Web“ erfolgt. Die Speicherkapazitäten der genutzten Medien wachsen ständig, Moores Gesetz, nach dem sich die Komplexität integrierter Schaltkreise mit minimalen Komponentenkosten etwa alle zwei Jahre verdoppelt, scheint nach wie vor zu gelten. Dies geht einher mit einer Miniaturisierung der eingesetzten Hardware.

Begleitet wird dies auf der gesellschaftlichen Ebene von einer nahezu grenzenlosen Akzeptanz der Datenverarbeitungsechnik und der damit einhergehenden Kommunikationsstrukturen: Die Zahl der Internetnutzer nähert sich immer stärker der Einwohnerzahl an; immer mehr Lebensbereiche werden virtualisiert. Das sog. „Web 2.0“, die interaktive Nutzung des Webs, führt zu einer Veränderung dessen, was wir bisher als Privatsphäre erlebt haben. Virtuelle soziale Netzwerke (wie z.B. MySpace, Xing, studi.vz etc.) verstärken diese Tendenzen.

Die öffentliche Verwaltung und sonstige öffentliche Stellen können sich dem Trend der Virtualisierung nicht verschließen: Webportale werden zu ihren unerlässlichen Aktionsfeldern. Neue Formen der modernen Technik werden entwickelt: Stichworte sind hier die großen Kartenprojekte, insbesondere der Bundesregierung (Gesundheitskarte und elektronischer Einkommensnachweis) aber auch die sog. Personenkennzeichen wie die einheitliche Steueridentifikationsnummer, die LKW-Mautdatenerfassung, die automatisierte Kennzeichenerfassung für polizeiliche Zwecke, das Projekt der Online-Durchsuchung für Zwecke der inneren Sicherheit und der Verknüpfung von Videoerfassungen für polizeiliche Zwecke.

Die Zahl der Baustellen im Datenschutzbereich ist also groß. Und wie immer in diesen Fällen, kann es nicht genug Facharbeiter und Instandhaltungskräfte geben, um diese Baustellen zu betreuen und den Bau (des Datenschutzes) insgesamt voranzubringen. Der LfD versucht dieser Situation auf unterschiedliche Weise Rechnung zu tragen:

Er hat – erstmals für das Jahr 2008 – einen Wissenschaftspreis ausgelobt, um Nachwuchswissenschaftler an rheinland-pfälzischen Hochschulen und Forschungseinrichtungen zu motivieren, sich verstärkt mit datenschutzrechtlichen Fragestellungen in den dafür in Betracht kommenden Fächern auseinanderzusetzen. Dies gilt für den geistes- und sozialwissenschaftlichen Bereich ebenso wie für den mathematisch-naturwissenschaftlichen. Der LfD hat dafür die Unterstützung der Hochschulen und der Regierung des Landes erhalten (s. Tz. 24.3).

Der LfD hat außerdem damit begonnen, die große Zahl der behördlichen Datenschutzbeauftragten zu einem Netzwerk zusammenzuschließen, um ihnen eine effektivere Arbeit in ihrem Verantwortungsbereich zu ermöglichen. Die ersten Schritte wurden im kommunalen Bereich unternommen, die nächsten sind für den Schulbereich und die Justiz geplant. Dabei wird sich der LfD auch dafür einsetzen, dass den behördlichen Datenschutzbeauftragten das notwendige Zeitbudget zur Verfügung gestellt wird, um die ihnen übertragenen Aufgaben auch ordnungsgemäß wahrnehmen zu können.

Des Weiteren wird der LfD seinen Teil dazu beitragen, dass die Angehörigen der sog. Online-Generation, insbesondere die Schüler, befähigt werden, verantwortungsvoller mit ihren Daten und denen von Dritten umzugehen, wenn sie das Internet und die sonstigen modernen Medien nutzen. Zu diesem Zweck ist mit dem MBWJK eine enge Zusammenarbeit bei der Umsetzung des Programms „Medienkompetenz macht Schule“ vereinbart.

Diese Zusammenarbeit soll erstmals am 28.1.2008 nach außen dokumentiert werden. An diesem Tag, der vom Europarat zum Europäischen Datenschutztag bestimmt worden ist, werden das MBWJK und der LfD eine gemeinsame zentrale Veranstaltung für Rheinland-Pfalz unter dem Motto „Denn sie wissen nicht, was sie tun – Datenschutz in der Online-Generation“ in der

Akademie der Wissenschaften und der Literatur in Mainz durchführen (s. Tz. 8.1.2). Bei der Veranstaltung, an der Vertreter des Landes, des Bundes und der Europäischen Union teilnehmen werden, soll zum Ausdruck gebracht werden, dass den Gefahren, die mit der Nutzung vor allem des Internets verbunden sind, nicht – jedenfalls nicht in erster Linie – durch normative Maßnahmen zu begegnen ist, sondern durch Erziehung und Information.

Jeder Nutzer des Internets ist zwar selbst dafür verantwortlich, in welchem Umfang er persönliche Daten preisgibt. Überwiegend fehlt den Betroffenen aber die Kenntnis davon, dass jede Nutzung des Internets persönliche Spuren im Netz hinterlässt, die auch nach Jahren und Jahrzehnten noch feststellbar sind. Insoweit muss bei den Bürgern ein Bewusstsein dafür geschaffen werden, dass das Internet ein ewiges Gedächtnis hat und dass dies nicht nur mit Gefahren für unsere Gesellschaft, sondern für jeden Einzelnen verbunden ist.

In diesem Kontext haben die Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe eingerichtet, die unter Federführung von Rheinland-Pfalz entsprechende Konzepte erarbeiten soll. Sie wird ihre Arbeit im März 2008 aufnehmen.

Schließlich wird der LfD auch seine Öffentlichkeitsarbeit ausweiten und dabei den Schwerpunkt insbesondere auf solche Initiativen legen, die geeignet sind, das Datenschutzbewusstsein in der Bevölkerung zu heben. Die Bandbreite der geplanten Aktivitäten reicht dabei von Informationsveranstaltungen bis zu einer entsprechenden Ergänzung und Überarbeitung der Homepage des LfD.

Der Ausblick am Ende des Tätigkeitsberichts zeigt also, dass es in den kommenden Jahren darum gehen wird, zusätzlich zu den bisher wahrgenommenen Aufgaben die institutionellen Ressourcen des Datenschutzes besser zu nutzen und die Möglichkeiten des Selbstdatenschutzes stärker als bisher zu aktivieren.

Insbesondere was den Selbstdatenschutz anbelangt, also die Verantwortung eines jeden für sein datenschutzrelevantes Verhalten, wäre es hilfreich, wenn die Zuständigkeiten für den öffentlichen und den privaten Datenschutz bei einer Stelle gebündelt würden. Auf diese Weise könnte den neuen Gefahren für den Datenschutz effektiver begegnet werden. Während nämlich zu Beginn der Datenschutzzeit in erster Linie der Staat als Bedrohung für die Privatsphäre der Bürger gesehen wurde, gehen entsprechende Gefahren mittlerweile offensichtlich mindestens in gleicher Weise von privaten Unternehmen aus. Ihr Interesse an den Daten ihrer Kunden dürfte mittlerweile größer sein, als der Datenbedarf staatlicher Stellen.

Anlage 1

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechts. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechts um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

Anlage 2

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internetprovider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internetnutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z.B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefaxsendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden. Mit einem Quickfreeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

Anlage 3

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung").

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die BA und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anlage 4

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

Anlage 5

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Telefonieren mit Internettechnologie (Voice over IP – VoIP)

Die Internettelefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internettechnologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internettechnologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internetprotokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdatenverkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Anlage 6

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u.a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Anlage 7

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 – Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

Anlage 8

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 15. Dezember 2005 – Sicherheit bei E-Government durch Nutzung des Standards OSCI

In modernen E-Government-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheitsstandard für E-Government-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in E-Government-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anlage 9

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 – Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z.B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anlage 10

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 – Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anlage 11

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 – Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt – einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Anlage 12

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 – Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internetprovider auch über – durch das Fernmeldegeheimnis geschützte – Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internetprovider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internetanbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung wirtschaftlicher Interessen – zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anlage 13

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 – Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in E-Government-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 14

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 – Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der "Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der "Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 15

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 – Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz – BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat – sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.
- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anlage 16

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 – Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- Kennzeichnungspflicht Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- Keine heimliche Profilbildung Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.
- Vermeidung der unbefugten Kenntnisnahme Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- Deaktivierung Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 17

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 – Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben“ ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten: Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen „Bildungsregisters“ nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Anlage 18

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z.B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.
- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss statt dessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.
- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.
- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.
- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.
- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.
- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.
- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

Anlage 19

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z.B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt um so mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Softwareupdates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

Anlage 20

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

Anlage 21

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

Anlage 22

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

Anlage 23

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 – Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

Anlage 24

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. Juni 2007 – Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, statt dessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichten und Aufbewahren von Identitätsnachweisen aller Personen, die Prepaidprodukte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internetcomputern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.