LANDTAG RHEINLAND-PFALZ
14. Wahlperiode

Drucksache 14/4660
14. 11. 2005

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Zwanzigster Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 2003 bis 30. September 2005

Inhaltsverzeichnis

Dem Präsidenten des Landtags mit Schreiben vom 10. November 2005 zugeleitet. Der Bericht wurde in der Kommission beim Landesbeauftragten für den Datenschutz nach § 26 Abs. 3 Satz 4 Landesdatenschutzgesetz vorberaten.

Druck: Landtag Rheinland-Pfalz, 16. Januar 2006

Seite

Seite

Seite

Seite

Anlagen

Abkürzungen

ABl.	Amtsblatt der Europäischen Gemeinschaften
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ArbGG	Arbeitsgerichtsgesetz
ArbzG	Arbeitszeitgesetz
AufenthG	Aufenthaltsgesetz
AuslG	Ausländergesetz
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BeamtVG	Beamtenversorgungsgesetz
BfD	Bundesbeauftragter für den Datenschutz
BFH	Bundesfinanzhof
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
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
BZRG	Bundeszentralregistergesetz
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	zirka
DIZ	Daten- und Informationszentrum Rheinland-Pfalz
DNA	Desoxyribonuclein acid (acid = Säure)
DNA-IFG	DNA-Identitätsfeststellungsgesetz
Drs.	Drucksache
DSO-LT	Datenschutzordnung des Landtags Rheinland- Pfalz
DVBl.	Deutsches Verwaltungsblatt
EG	Europäische Gemeinschaften
EGV	Vertrag über die Europäische Gemeinschaft
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
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
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes und der Länder beim Bundeskriminalamt
ISM	Ministerium des Innern und für Sport
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
JM	Ministerium der Justiz
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KpS	Kriminalpolizeiliche personenbezogene Sammlungen – Kriminalakten –
KV	Kassenärztliche Vereinigung
KWG	Kommunalwahlgesetz
KWO	Kommunalwahlordnung
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LArchG	Landesarchivgesetz
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

LPersVG	Landespersonalvertretungsgesetz
LRG	Landesrundfunkgesetz
LSG	Landessozialgericht
LSJV	Landesamt für Soziales, Jugend und Versorgung
LT-Drs.	Landtagsdrucksache
Lufa	Landwirtschaftliche Untersuchungs- und Forschungs-Anstalt Speyer
LV	Landesverfassung für Rheinland-Pfalz
LVA	Landesversicherungsanstalt
LVerfSchG	Landesverfassungsschutzgesetz
LVwVfG	Landesverwaltungsverfahrensgesetz
MADG	Gesetz über den MAD
MASFG	Ministerium für Arbeit, Soziales, Familie und Gesundheit
m. a. W.	mit anderen Worten
MDK	Medizinischer Dienst der Krankenversicherung
MEK	Mobiles Einsatzkommando
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
MMR	Multimedia und Recht
MRRG	Melderechtsrahmengesetz
n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
o. ä.	oder ähnliches
OFD	Oberfinanzdirektion
o. g.	oben genanntes
ÖGdG	Landesgesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PBefG	Personenbeförderungsgesetz
PC	Personalcomputer
POG	Polizei- und Ordnungsbehördengesetz
POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
PostG	Postgesetz
PStG	Personenstandsgesetz
PsychKG	Landesgesetz für psychisch kranke Personen
RdNr.	Randnummer
RDV	Recht der Datenverarbeitung
RIVAR	Rheinland-pfälzisches Informations-, Vorgangsbearbeitungs-, Auswerte- und Recherchesystem
RSAV	Risikostruktur-Ausgleichsverordnung
s.	siehe
SchulG	Schulgesetz
SDÜ	Schengener Durchführungsübereinkommen
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
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
Tb.	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
Tz.	Textziffer
u. a.	unter anderem
UIG	Umweltinformationsgesetz
UstG	Umsatzsteuergesetz
u. U.	unter Umständen
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
z. B.	zum Beispiel
ZPO	Zivilprozessordnung
z. T.	zum Teil

Glossar technischer Begriffe

ActiveX	Eine Software-Technologie von Microsoft. ActiveX erlaubt es, sogenannte Applets zu erstellen, die vom *Server* auf den Rechner des Internet-Nutzers übertragen und dort ausgeführt werden. Die Applets können dabei grundsätzlich auf alle Ressourcen des Zielrechners zugreifen, d. h. gegebenenfalls Daten lesen, löschen oder verändern.
ADABAS/Natural	Ein – überwiegend im Großrechnerbereich eingesetztes – Verfahren zur Verwaltung und Auswertung von in einer Datenbank gespeicherten Informationen (siehe auch *Relationales Datenbanksystem*).
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*.
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 Web-Seiten, d. h. von Inhalten im Internet. Gängige Browser sind der Microsoft Internet Explorer und der Netscape Navigator.
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 Rescue Teams, einer Sicherheitsorganisation für das Internet. Ein deutschsprachiges CERT existiert für das Deutsche Forschungsnetz (DFN) unter der Internet-Adresse 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 Internet-Dienstes, 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.
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.
DICOM	Im Bereich der Medizin genutztes Kommunikationsprotokoll für die Übertragung von Radiologiedaten.
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. Internet-Dienst der *IP-Adressen* in leichter zu merkende Rechnernamen umsetzt (z. B. 192.168.100.010 in www.firma.de).
DNS-Server	Rechner bzw. Programme, welche DNS-Dienste bereitstellen.
Download	Herunterladen von Daten aus dem Internet auf das eigene IT-System.
DSS	Digital Signature Standard. Ein kryptografisches Verfahren für die *digitale 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 *Hash-Verfahren* 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.
Fax-Server	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 Signaturschlüssel-Inhabers 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 Standard Query Language.
FTP	File Transfer Protokoll. Speziell auf die Übertragung von Datenbeständen ausgerichtetes Kommunikationsprotokoll aus der Familie der Internet-Protokolle.
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.

Hash-Verfahren	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 *digitalen Signatur* für den Nachweis der Integrität einer Nachricht benötigt.
Hashwert	Prüfsumme als Ergebnis eines Hash-Vorgangs.
Homepage	Start- und Begrüßungsseite eines Internet-Angebotes. 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 *Web-Seiten* 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 *Web-Seiten* auf dem lokalen System oder im Internet.
HTTP	Hypertext Transfer Protocol. Internet-Protokoll zur Darstellung vom *HTML*-Seiten via *Browser*.
Hyperlink	siehe *HTML*. Verweis auf andere Web-Seiten 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	Unversehrtheit und Vollständigkeit der in elektronischer Form gespeicherten oder übermittelten Daten. Der Nachweis der Integrität einer elektronischen Nachricht, z. B. mittels *Hash-Verfahren* gewährleistet, dass diese während der Übertragung nicht verändert wurde.
Internet-Adresse	Angabe, unter welcher Bezeichnung Informationen oder Dienste im Internet angesprochen werden können. Die Internet-Adresse wird meist als URL (Unique Ressource Locator) angegeben. Eine typische Internet-Adresse ist z. B. http://www.datenschutz.rlp.de.
IP-Adresse	Internet Protocol-Adresse. Numerische Angabe für die eindeutige Bezeichnung eines Rechners im Internet (z. B. 192.168.100.010); 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-Karte	PC-seitige Komponente (Steckkarte) zum Anschluss an das ISDN-Netz.
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.
Java-Script	Eine von den Firmen SUN und Netscape entwickelte Makrosprache. Die damit erstellten Anweisungen (scripts) werden vom Browser des Client-Rechners 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.
Krypto-Box	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.
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.
Mail-Gateway	Vermittlungsrechner, der die Entgegennahme und Weiterleitung von E-Mail-Nachrichten steuert.
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 erfolgen.
OCR	Optical Character Recognition. Verfahren zur automatisierten 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 Versuch, 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.
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.
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.*
SAN	*Storage Area Network.*
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 Netzwerk-Betriebssystem 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 Mail-Servers 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.
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.
Storage Area Network	Datennetzwerk zur Anbindung von Speicher- und Sicherungsmedien an Serversysteme.
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 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. Standard-Kommunikations-*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 Paket-Empfangs. 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.
Telebox 400	E-Mail-Verfahren der Deutschen Telekom AG auf der Basis des *X.400*-Protokolls.
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.
Trust-Center	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*.
Verzeichnisdienst	Serverdienst, 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 nutzende Netze gegeneinander abzuschotten.
Voice-over-IP	siehe *VoIP*.
VoIP	„Voice-over-IP“ Eine Technologie auf Basis des Internet-Protokolls, 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.
Web-Seite	Seite eines Angebots im *World Wide Web.*
WEP	*Wired Equivalent Privacy.*
Wired Equivalent Privacy	Verschlüsselungsmethode für *WLAN*, welche zur Sicherung der Vertraulichkeit der Kommunikation zwischen den WLAN-Komponenten eingesetzt wird. Aufgrund von Schwachstellen in der Implementierung mittlerweile nicht mehr als ausreichend sicher angesehen.
Wireless Fidelity Protected Access	Verschlüsselungsmethode für *WLAN*, welche einen höheren Sicherheitsstandard als WEP darstellt.
Wireless Local Area Network	Lokales Datennetzwerk, welches zur Übertragung der Datenpakete Funktechnik an Stelle von leitungsgebundenen Übertragungswegen einsetzt.
WLAN	*Wireless Local Area Network.*
World 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.*
WPA	*Wireless Fidelity Protected Access.*
WWW	siehe *World Wide Web.*
X.400	Ein Übertragungsprotokoll für den Austausch elektronischer Nachrichten (Elektronische Post).
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.

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

1. Vorbemerkung

Grundfragen des Datenschutzes

Freiheit und Sicherheit, so heißt es regelmäßig beispielsweise in Grundsatzerklärungen der Europäischen Union, seien Begriffe, die sich gegenseitig bedingen: Ohne Sicherheit gäbe es keine Freiheit, ohne Freiheit sei Sicherheit wertlos. Diese Aussage darf aber nicht dazu verführen zu glauben, es handele sich hier um ein sich selbst regulierendes System und man könne ruhig darauf vertrauen, dass sich ein angemessenes Verhältnis beider Ziele von selbst einstellen werde. Das Sicherheitsbedürfnis hat sehr wirksame soziale Agenten, während sich das Freiheitsbedürfnis gelegentlich nur mühsam und in eher verlustreichen Abwehrkämpfen durchsetzen kann. Dies spürt der Datenschutzbeauftragte nicht selten.

Allerdings ist Pessimismus nicht angebracht. Unter Datenschützern und „Bürgerrechtlern“ wird häufig ein Bild der ständig weiter zurückgedrängten Bürgerrechte gemalt; umstritten ist dann nur noch die Frage, ob in der aktuellen Entwicklung der Datenschutz durch die Wirtschaft oder durch den Staat mehr gefährdet sei.

Für die vorgeblich umfassende Bereitschaft des Staates, in Freiheitsrechte einzugreifen, sei ein übersteigertes Sicherheitsbedürfnis verantwortlich, das durch den Topos der Terrorismusbekämpfung nahezu entfesselt sei. In diesen Zusammenhang gehören die Diskussionen um die Rasterfahndung, um Abhörmaßnahmen in Wohnungen zu strafverfolgenden und vorbeugenden Zwecken und um die Erweiterung der DNA-Analysebefugnisse. Auch die Einführung des Personalausweises mit biometrischen Merkmalen gehört in diesen Kontext.

Hinzu komme die umfassende Wissbegier des Staates in seiner Eigenschaft als Steuereinnehmer (Stichworte: Zentraler Kontenzugriff, Geldwäscheverdachtsanzeigen, Autobahnmaut) und Leistungserbringer (besonders auch in Zusammenhang mit Hartz IV und dem Jobcard-Projekt) sowie als Organisator des Gesundheitswesens (z. B. Gesundheitskartenprojekt).

Andererseits wird gewarnt, viel gefährlicher sei die Wirtschaft. Sie locke den Verbraucher mit Rabattkarten, intimste Gewohnheiten, die sich im Güterverbrauch spiegeln, zu offenbaren. Verbraucherprofile, die ungeahnte Beeinflussungsmöglichkeiten eröffneten, seien das Ergebnis. Hinzu kämen Kredit-Scoring, Kreditschutzdateien und sonstige Datensammlungen über die tatsächliche oder vermeintliche Konsumkraft des Bürgers (oder deren Fehlen), so dass für den Einzelnen keine Rede mehr sein könne von Selbstbestimmung in Bezug auf seinen Datenschatten.

Außerdem werde die informationelle Einkreisung des Bürgers, gleich ob staatlicher oder privater Natur, durch die neuen technischen Entwicklungen verschärft: vom RFID-Einsatz auf Waren und im Pass oder Personalausweis bis zu den neuen Entwicklungen des pervasive Computing, von der exponentialen Weiterentwicklung der Kapazitäten der Speichermedien ganz zu schweigen, sei alles darauf angelegt, die Bürgerrechte zu schwächen. Wenn die Video-Überwachung (mit den neuen Möglichkeiten der Gesichtserkennung) im Rahmen des Hausrechts und in öffentlich zugänglichen Räumen in die Betrachtung einbezogen werde, sei die Volkszählung von 1983 eine Kleinigkeit, verglichen mit der Bedrohung durch allgegenwärtige Überwachung und Erfassung.

Der LfD sieht demgegenüber weder im technischen Fortschritt noch in der Entwicklung der staatlichen oder privaten Datenverarbeitung oder in der Gesetzgebung der letzten Jahre den Tod des Datenschutzgrundrechts. Wenn auch alle beschriebenen Erscheinungen zumindest der Tendenz nach existieren, so sind sie weder im Einzelnen noch in ihrer Gesamtheit ein Indiz für einen macht- und einflusslosen Datenschutz. Es ist zwar richtig, dass die Gefahrenvorsorge und die Gefahrenabwehr immer mehr in das Vorfeld konkreter Gefahren verlagert werden und dass damit Grundrechtseingriffe möglich geworden sind, die vor den entsprechenden Gesetzesänderungen nicht möglich waren. Hierbei handelt es sich um eine stetige Tendenz. Dies bedeutet aber keineswegs, dass wir etwa eine Entwicklung hin zum „Feindstrafrecht“ bzw. zu einer „Guantanamoisierung“ des Rechts erleben würden; eine solche Einschätzung wäre eine grobe Verzerrung der Realität. Allerdings ist auch im Kampf gegen den Terrorismus das Nietzsche-Wort zu bedenken: „Wer mit Ungeheuern kämpft, mag zusehn, daß er nicht dabei zum Ungeheuer wird.“

In den datenschutztechnisch orientierten Diskussionen fällt eine merkwürdig widersprüchliche Haltung gegenüber dem technischen Fortschritt auf: zum einen sei er geeignet, immer umfassender Persönlichkeitsmerkmale zu erheben und zu speichern; beispielsweise wird das Horrorgemälde einer allgemeinen Gendatenbank und ihrer nahezu unbeschränkten Nutzbarkeit gemalt; zum andern wird aber auf die Unzuverlässigkeit und Fehleranfälligkeit der Technik verwiesen (besonders z. B. im Zusammenhang mit biometrischen Systemen der Personenidentifizierung).

Nach der Einschätzung des LfD hat der Datenschutz in allen genannten Bereichen den staatlichen Tätigkeiten wesentliche Schranken gesetzt und zu einem Ausgleich zwischen den relevanten Staatsaufgaben und den Grundrechten beigetragen, der bislang als angemessen zu bezeichnen ist. Auch für den Datenschutz gilt: „Wo aber Gefahr ist, wächst das Rettende auch.“ Neue Instrumente des Datenschutzes, verfassungsgerichtliche Leitentscheidungen, datenschutzfreundliche Technik, die Kenntnis der Bürger über Möglichkeiten des „Selbstdatenschutzes“ – alles das hat dazu beigetragen, dass die eingangs geschilderten Bedingungen beherrschbar geblieben sind und nicht zu einer Situation der Recht- und Machtlosigkeit der Bürger geführt haben. In diesem Sinn haben nicht nur die Datenschutzbeauftragten des Bundes und der Länder gewirkt, sondern ganz wesentlich auch grundrechtsbewusste Politiker und Mitarbeiter in Ministerien und Verwaltungen. Dies wird der folgende Bericht im Einzelnen an vielen Stellen belegen.

Richtig ist allerdings aus der Sicht des LfD, dass Wachsamkeit und Aufmerksamkeit gegenüber den Gefährdungen der Persönlichkeitsrechte und besonders des Datenschutzgrundrechts weiterhin geboten sind und dass insbesondere im Bereich der privaten Wirtschaft die Effizienz der bestehenden Schutzregelungen intensiv geprüft und beobachtet werden muss.

2. Weiterentwicklung des Datenschutzrechts

2.1 Unabhängigkeit der Datenschutzkontrolle

Der LfD hält die in Rheinland-Pfalz und anderen Bundesländern bewährte Trennung des Datenschutzes im öffentlichen und im privaten Bereich nach wie vor für notwendig. Mögen die technischen Bedingungen sich weitgehend gleichen, so ist die Unterscheidung zwischen Grundrechtsschutz gegenüber dem Staat und Datenschutz zwischen Privaten nicht zu verwischen. Die vom Bundesverfassungsgericht geforderte Unabhängigkeit des LfD ist in Rheinland-Pfalz organisatorisch vorbildlich geregelt. Wenn die Europäische Kommission die nach der Europäischen Datenschutzrichtlinie geforderte völlige Unabhängigkeit sämtlicher Datenschutzkontrollstellen im Falle der Aufsichtsbehörden für den privaten Bereich vermisst und damit eine Verletzung von EG-Recht rügt, so kann der LfD dem nicht folgen. Mit der Bundesregierung stimmt er überein, dass auch nach EG-Recht allein die funktionelle Unabhängigkeit gefordert ist, wie sie beispielsweise auch bei den Datenschutzbeauftragten der Kirchen und der Rundfunkanstalten gewährleistet wird. Eine der richterlichen Unabhängigkeit vergleichbare, nicht der Rechtsaufsicht unterliegende Unabhängigkeit auch der Datenschutz-Aufsichtsbehörden, die nicht nur Kontrollfunktionen, sondern unmittelbare Eingriffsbefugnisse gegenüber natürlichen und juristischen Personen des Privatrechts haben, setzt eine Änderung der Verfassung voraus, sofern sie überhaupt verfassungsänderungsfähig ist (Art. 79 Abs. 3, 20 Abs. 3 GG).

2.2 Überblick

Das Landesdatenschutzgesetz wurde im Berichtszeitraum nicht geändert.
Allerdings gab es im bereichsspezifischen Datenschutzrecht Entwicklungen. So ist das Polizei- und Ordnungsbehördengesetz erneut im Bereich der datenschutzrelevanten Bestimmungen geändert worden, s. Tz. 5.1. Auch die StPO ist in wesentlichen Punkten, den Bestimmungen über die akustische Wohnraumüberwachung (§ 100 c StPO) und über die molekulargenetischen Analysen im Strafverfahren (insbesondere § 81 e StPO) neu gefasst worden (s. Tz. 7.1).

Auf der Ebene des Landes sind weiterhin neben dem Schulgesetz (s. Tz. 8.1.1) das Meldegesetz (s. Tz. 4.1), das Landesbeamtengesetz (§ 61 a, s. Tz. 10.2.1 und 10.2.2) sowie das Brand- und Katastrophenschutzgesetz (s. Tz. 18.3) zu nennen.

Auf Bundesebene sind insbesondere die Abgabenordnung mit ihren Regelungen zum Kontenzugriff (§ 93 a und b AO, s. Tz. 13.1) sowie das Zweite Buch des Sozialgesetzbuchs unter dem Stichwort „Hartz IV“ (s. Tz. 11.1) zu erwähnen.

Das Telekommunikationsrecht ist auch im Bereich der datenschutzrelevanten Regelungen weiter entwickelt worden, s. Tz. 19.1.

Das Bundesdatenschutzgesetz erfuhr keine substantielle Änderung im Berichtszeitraum. Hier gibt es allerdings weiterhin Bestrebungen zur Einführung der sogenannten „zweiten Stufe“ der Novellierung, die in erster Linie das Datenschutzaudit-Verfahren einführen soll.

An allen Novellierungsvorhaben war der LfD in der Form beteiligt, dass er gegenüber den Landesressorts bzw. dem BfD Stellung genommen hat.

Schließlich ist auf die Beschlüsse der 27. Internationalen Konferenz der Datenschutzbeauftragten, die in Montreux (Schweiz) vom 14. bis 16. September 2005 stattgefunden hat, hinzuweisen (s. Anlage 20). Hervorzuheben ist hier insbesondere die „Erklärung von Montreux“, mit der an die Vereinten Nationen appelliert worden ist, ein internationales Abkommen zum Datenschutz in Angriff zu nehmen.

2.3 Informationsfreiheitsgesetz

Ob das Informationsfreiheitsrecht überhaupt ein Teil des „Datenschutzrechts“ ist, ist umstritten. Nur nach einem bestimmten Verständnis des Datenschutzrechts, nämlich wenn man es als „Informationsverteilungsrecht“ auffasst, als Teil einer „Datenverkehrsordnung“, ist diese Sicht der Dinge angemessen. Aus der Sicht des Datenschutzes als Grundrechts- und Persönlichkeitsschutz ist das Informationsfreiheitsrecht dagegen eher als Gefährdungspotential und als Antithese zu sehen.

Unabhängig von dieser Grundsatzfrage ist das Informationsfreiheitsrecht in jedem Fall Gegenstand der besonderen Aufmerksamkeit der Datenschutzbeauftragten. Nunmehr ist auf der Ebene des Bundes ein entsprechendes Gesetz erlassen worden (Gesetz zur Regelung des Zugangs zu Informationen des Bundes – IFG – vom 5. September 2005, BGBl. I 2005, 2722), das zum 1. Januar 2006 in Kraft treten wird. Damit ist eine wesentliche Voraussetzung erfüllt, die seitens der Landesregierung in der Vergangenheit für entsprechende Initiativen auf der Ebene des Landes genannt worden ist. Allerdings sind konkrete gesetzgeberische Initiativen derzeit nicht ersichtlich. Nach den Erfahrungen des LfD ist es schwierig und aufwändig genug, den Auskunftsanspruch der von Datenverarbeitungen Betroffenen zu realisieren. Die Schaffung weiterer gesetzlicher Grundlagen für Auskunftsansprüche gegenüber der

Verwaltung wird die Persönlichkeitsrechte der Betroffenen nicht unmittelbar stärken. Dennoch sieht der LfD die hier stattfindende Entwicklung als unvermeidbar an; er ist zuversichtlich, dass ein den relevanten und schützenswerten Interessen gerecht werdendes Ergebnis erzielbar ist. In diesem Zusammenhang hat der LfD verschiedentlich gegenüber interessierten Privatpersonen und Organisationen Stellung genommen; er hat seine Position auch in einer Anhörung des sächsischen Landtags zu einem dort eingebrachten entsprechenden Gesetzentwurf der PDS-Fraktion vorgetragen.

3. Datenschutz in Europa

3.1 Europäischer Datenschutzbeauftragter

Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft (vgl. hierzu im Einzelnen 18. Tb., Tz. 3.2) sieht die Einrichtung eines Europäischen Datenschutzbeauftragten vor. Er ist eine unabhängige Kontrollbehörde und stellt gem. Art. 41 Abs. 2 vorgenannter Verordnung sicher, dass die Grundrechte und -freiheiten natürlicher Personen, insbesondere das Recht auf Schutz der Privatsphäre, bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft eingehalten werden. Des Weiteren berät er die Organe und Einrichtungen der Gemeinschaft in allen Fragen, die die Verarbeitung personenbezogener Daten betreffen. Art. 46 Buchstabe a regelt, dass der Datenschutzbeauftragte von sich aus oder aufgrund einer Beschwerde Untersuchungen durchführt und die betroffenen Personen über die Ergebnisse seiner Untersuchungen informiert.

Nach der Entscheidung, eine Untersuchung einzuleiten, erhält der Datenschutzbeauftragte eine Reihe von Befugnissen (vgl. Art. 47); beispielsweise kann er
- die Berichtigung, Sperrung, Löschung oder Vernichtung aller unzulässig verarbeiteten Daten anordnen,
- den für die Verarbeitung Verantwortlichen verwarnen,
- das Europäische Parlament, den Rat und die Kommission mit der Angelegenheit befassen
- sowie die Verarbeitung vorübergehend oder endgültig verbieten.

Die genaue Tätigkeitsbeschreibung des Europäischen Datenschutzbeauftragten ist veröffentlicht worden (Fundstelle: Amtsblatt der EG C 224A vom 20. September 2004).

Es ist zu erwarten, dass strittige Fälle vor den Gerichtshof der Europäischen Gemeinschaften gebracht werden. Denn nach Art. 32 kann gegen die Entscheidungen des Datenschutzbeauftragten Klage beim Gerichtshof der Europäischen Gemeinschaften erhoben werden. Auch der Datenschutzbeauftragte kann den Gerichtshof anrufen sowie dort anhängigen Verfahren beitreten.

Der frühere Vorsitzende der Niederländischen Datenschutzkommission Peter J. Hustinx wurde im Dezember 2003 vom Europäischen Parlament und dem Rat der Europäischen Union für die Amtszeit von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt und hat sein neues Amt im Januar 2004 angetreten. Er arbeitet als gleichberechtigtes Mitglied in der Art. 29-Gruppe (vgl. Tz. 3.3) mit. Seine Internet-Adresse lautet: www.edps.eu.int.

3.2 Der gläserne Passagier

Als Folge der Anschläge vom 11. September 2001 trat im März 2003 in den USA ein Gesetz in Kraft, das allen ausländischen Fluglinien bei Flügen in die Vereinigten Staaten vorschreibt, ihr Buchungssystem für die US-Zollbehörden zu öffnen. Es gab eine Vereinbarung zwischen der EU-Kommission und den USA, in der Einzelheiten des Datenzugriffs durch US-Behörden festgelegt wurden. Die Bestimmungen der EG-Datenschutzrichtlinie, die bei Datenübermittlungen außerhalb der Europäischen Union hohe Voraussetzungen vorsehen, sind dabei offensichtlich außer Acht gelassen worden. Daraufhin forderte das Europäische Parlament in einem Beschluss die EU-Kommission auf, in Verhandlungen mit den US-Zollbehörden hinsichtlich der Fluggast-Datenweitergabe die Bestimmungen der EG-Datenschutzrichtlinien zu berücksichtigen, um den rechtswidrigen Zustand zu beenden. Nach langwierigen und schwierigen Verhandlungen zwischen der EU-Kommission und dem US-Heimatschutzministerium hat der Rat der Europäischen Union am 17. Mai 2004 mit den USA ein bilaterales Abkommen bezüglich der Übermittlung von Passagierdaten durch die Fluggesellschaften an die amerikanischen Zoll- und Grenzschutzbehörden geschlossen. Vorausgegangen war die am 14. Mai 2004 getroffene Feststellung der EU-Kommission, wonach das von den US-Behörden gewährleistete Schutzniveau angemessen sei.

Dieses Abkommen hat unmittelbare Auswirkungen auf in der Europäischen Union stattfindende Datenverarbeitungen. In den Passagierdatenbanken werden z. B. Name, Reiseverlauf, Buchungsstelle, Hotel- und Mietwagenreservierungen, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, notwendige Reisevorkehrungen wegen Behinderung oder Erkrankung eines Fluggastes und Essenswünsche gespeichert. Die gespeicherten Daten sind teilweise sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse Anschauungen ermöglichen. Die ursprünglich seitens der USA vorgesehene Speicherfrist von 50 Jahren konnte inzwischen auf 3 ½ Jahre reduziert werden. Die Behörden der USA erhalten die Passagierdaten im sog. „Pull-Verfahren“, d. h. durch Zugriff auf die Reservierungssysteme der Fluggesellschaften. Sie greifen dabei auf den kompletten Datensatz zu, der zu den einzelnen Passagieren vorliegt.

Während der Verhandlungen haben sich auch die Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung zur Übermittlung von Flugpassagierdaten an US-Behörden (s. Anlage 2) zu Wort gemeldet. Darin wird die Problematik dargestellt und ein angemessener Schutz der Reisenden, was ihre Persönlichkeitsrechte anbelangt, gefordert. Ebenso hat die Gruppe nach Art. 29 der EG-Datenschutzrichtlinie (vgl. Tz. 3.3) mehrfach Stellung genommen und praktische Maßnahmen für dringend erforderlich gehalten, um die Eingriffe in die Rechte der Passagiere so gering wie möglich zu halten. Dazu gehört die Forderung, dass die Fluggesellschaften die Datenübermittlung so schnell wie möglich vom „Pull-Verfahren“ auf ein „Push-Verfahren“ umstellen, wobei dann die Fluggesellschaften die vereinbarten Daten aktiv übermitteln.

Das Europäische Parlament hält auch das nachgebesserte Übereinkommen für unvereinbar mit den geltenden europarechtlichen Datenschutzbestimmungen und hat Klage vor dem Europäischen Gerichtshof erhoben. In diesem Verfahren wird nun überprüft, ob die Rechte der Fluggäste aufgrund der Angemessenheitsentscheidung sowie des Abkommens verletzt werden und eine Zustimmung des Parlaments zu dem Abkommen erforderlich gewesen wäre. Mit einer Entscheidung wird nicht vor Mitte 2006 gerechnet.

3.3 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Neben den Datenschutzbeauftragten der Mitgliedstaaten der EU gehören der Europäische Datenschutzbeauftragte (vgl. Tz. 3.1) der Art. 29-Gruppe als Mitglied sowie als nichtstimmberechtigtes Mitglied die Europäische Kommission an. Die Aufgaben und Tätigkeiten dieses unabhängigen europäischen Beratungsgremiums in Datenschutzfragen hat der LfD im 18. Tb. (Tz. 3.6) und 19. Tb. (Tz. 3.4) beschrieben. Im Berichtszeitraum hat sich die Gruppe wiederum mit einer weitgespannten Palette von Themen auseinandergesetzt.

Einige wichtige Dokumente (sog. Arbeitspapiere/WP) sind nachfolgend aufgeführt:

- WP 87
  Stellungnahme über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records – PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden;

- WP 89
  Stellungnahme zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung;

- WP 90
  Stellungnahme zu unerbetenen Werbenachrichten im Sinne von Artikel 13 der Richtlinie 2002/58/EG;

- WP 91
  Arbeitspapier über genetische Daten;

- WP 93
  Erklärung zu den Terroranschlägen in Madrid;

- WP 97
  Stellungnahme zur Unterrichtung von Fluggästen anlässlich der Übermittlung persönlicher Daten bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika.

Sämtliche Arbeitspapiere der Art. 29-Datenschutzgruppe sind im Internet unter http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/ abrufbar.

4. Meldewesen

4.1 Novellierung des Melderechts

In den letzten Jahren hat eine grundlegende Neuordnung des Meldewesens stattgefunden (vgl. zur Entwicklungsgeschichte 18. Tb., Tz. 4.1 und Tz. 21.2.1; 19. Tb., Tz. 21.2.5). Im Gegensatz zu dem früheren landeseinheitlichen Verfahren für das Meldewesen, das beim Landesrechenzentrum betrieben wurde, verfügen alle Meldebehörden inzwischen über ein eigenes Melderegister, das in eigener Verantwortung zur Erledigung der vor Ort anfallenden meldebehördlichen Aufgaben genutzt wird. Einzelne überörtliche meldebehördliche Aufgaben sollen daneben unter Nutzung des im Rahmen des Integrationssystems vorgehaltenen Gesamtbestandes der Grunddaten aller Melderegister weiterhin gemeinsam für alle 212 Meldebehörden in Rheinland-Pfalz zentral erledigt werden. In der Verantwortung des Landes wird daneben das Informationssystem betrieben, das der Polizei und anderen öffentlichen Stellen den automatisierten Abruf von Daten ermöglicht. Die inzwischen erfolgte Einführung des neuen Verfahrens hat – ebenso wie zahlreiche rahmenrechtliche Gesetzesänderungen auf Bundesebene – eine Änderung des Meldegesetzes notwendig gemacht. Die rechtlichen und technischen Rahmenbedingungen für diese Entwicklung sind mit dem LfD abgestimmt worden. Ihm wurde auch Gelegenheit gegeben, zu dem Entwurf eines Zweiten Landesgesetzes zur Änderung des Meldegesetzes bereits im Rahmen der Ressortabstimmung Stellung zu nehmen.

Ein wesentlicher Teil der Änderungen resultiert aus der Übernahme der Regelungen des Dritten Gesetzes zur Änderung des Melderechtsrahmengesetzes (vgl. hierzu die Darstellungen im 18. Tb., Tz. 4.2 und 19. Tb., Tz. 4.1). Hier hat der LfD nochmals auf die diesbezügliche Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. März 2001 hingewiesen (s. 18. Tb., Anlage 24). Einige dort benannte Kernforderungen der Datenschutzbeauftragten sind im Melderechtsrahmengesetz leider nicht berücksichtigt worden. Insbesondere wurde die einfache Melderegisterauskunft über das Internet nicht von der ausdrücklichen Einwilligung der Betroffenen abhängig gemacht. Vor dem Hintergrund, dass es sich hier um personenbezogene Daten handelt, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden, ist die vom Gesetzgeber getroffene Grundsatzentscheidung zu Gunsten einer Widerspruchslösung zu bedauern. Des Weiteren dürfen auch künftig Melderegisterauskünfte an politische Parteien zu Wahlwerbezwecken erteilt werden, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Auch hier hatten die Datenschutzbeauftragten eine Einwilligungsregelung gefordert.

Soweit hinsichtlich des zu übernehmenden Rahmenrechts noch ein Gestaltungsspielraum vorhanden war, hat der LfD – um den Schutz der Betroffenen beim Umgang mit ihren personenbezogenen Daten noch weiter zu verbessern – entsprechende Änderungsvorschläge unterbreitet, die größtenteils in den dem Landtag vorgelegten Gesetzesentwurf übernommen wurden. Sie betrafen u. a. die Verschlüsselung der Datenübertragung bei der Auskunft, die bedingte Auskunftspflicht der Vermieter sowie die Form der Bekanntmachung des Widerspruchsrechts bei der Auskunft über das Internet. Im Hinblick auf die rahmenrechtlichen Vorgaben ist die Melderegisterauskunft über das Internet von besonderer Bedeutung und wird nachfolgend dargestellt.

4.1.2 Die Online-Auskunft

In Anpassung an das Melderechtsrahmengesetz des Bundes sind in Rheinland-Pfalz die Rechtsgrundlagen für eine Online-Melderegisterauskunft geschaffen worden. Nunmehr können auch private Stellen oder Personen über das Internet einfache Melderegisterauskünfte (Vor- und Familienname, Doktorgrad und aktuelle Anschriften) erhalten. Diese Erweiterung hatte der LfD zunächst kritisch beurteilt. So gab es in der Vergangenheit immer wieder Verwechslungen bei der Auskunftserteilung aus dem Melderegister (vgl. z. B. 17. Tb., Tz. 4.10). In diesen Fällen wurde auch dann eine aktuelle Adresse mitgeteilt, wenn der Auskunftsbegehrende die Zielperson nicht eindeutig identifiziert hat. Wenn z. B. die Schreibweise des Namens oder das Geburtsdatum nicht mit dem im Melderegister gespeicherten Daten übereinstimmte, kam es vor, dass gleichwohl Auskunft erteilt wurde – teilweise unter Berichtigung der Angaben. Dies führte dazu, dass die Auskunft eine nicht tatsächlich angefragte Person betraf.

Mit der Neuregelung wird nun jedoch die dafür ursächliche mangelnde Sorgfalt in der manuellen Sachbearbeitung bei automatisierten Verarbeitungsformen (hier per Abruf über das Internet) programmtechnisch unterbunden. Dies geschieht dadurch, dass nach § 34 Abs. 2 Nr. 3 MG die Identität der betroffenen Person durch einen automatisierten Abgleich der im Auskunftsantrag angegebenen mit den im Melderegister gespeicherten Daten der betroffenen Person eindeutig festgestellt werden muss. Anderenfalls unterbleibt die Auskunft. Die beschriebene Verfahrensweise führt also unter den Gesichtspunkten der Datensicherheit und Datensparsamkeit zu einer Verbesserung des Schutzes personenbezogener Daten.

Die Einwohnerinnen und Einwohner haben das Recht, der Melderegisterauskunft an Private über das Internet zu widersprechen. Die Widerspruchserklärung ist gegenüber der Meldebehörde abzugeben. Auf die Eröffnung des Zugangs und das Widerspruchsrecht hat sie bei der Anmeldung sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Der Widerspruch bedarf keiner Begründung; die Bearbeitung erfolgt gebührenfrei.

Um den Regelungszusammenhang zu verdeutlichen, ist als Anlage 19 § 34 MG, der die Melderegisterauskunft an private Stellen und Personen betrifft, nebst auszugsweiser Entwurfsbegründung (LT-Drs. 14/4013) abgedruckt. Der dort in Absatz 4 erwähnte Internetzugang über ein sog. Portal soll es ermöglichen, eine Vielzahl einfacher Melderegisterauskünfte in sehr kurzer Zeit elektronisch abzurufen. Als Nutzende dieses Verfahrens werden Großkunden erwartet, die täglich Datenbestände aus dem Melderegister benötigen. Sofern diesbezüglich Interesse an der Wahrnehmung des angebotenen Verfahrens besteht, wird sich der LfD an dem zu erarbeitenden detaillierten Sicherheitskonzept für die Internetzugänge und Portale beteiligen.

4.1.3 Entwurf einer Informationssystemabrufverordnung

Im Zuge der Änderungen des rheinland-pfälzischen Meldegesetzes sollen die Regelungen über automatisierte Abrufe von Meldedaten seitens öffentlicher Stellen in einer Informationssystemabrufverordnung erweitert werden. Die Verordnung befindet sich gegenwärtig unter Beteiligung des LfD in der Ressortabstimmung. Von besonderer Bedeutung ist die detaillierte Festlegung des Datenschutzstandards für automatisierte Abrufe von Meldedaten. Hier wird es neben einer umfassenden Regelung zu den erforderlichen Sicherungsmaßnahmen auch eine 100 %-Protokollierung für Zwecke der Datenschutzkontrolle geben, wobei Aufbewahrung und Verwendung von Protokolldaten näher bestimmt werden.

Der LfD wird den Abstimmungsprozess weiterhin begleiten.

4.2 Meldedaten für den Südwestrundfunk

Im Berichtszeitraum gab es mehrere Anfragen von Gemeinden, bei denen es um Übermittlungsersuchen der Rundfunkgebührenbeauftragten des Südwestrundfunks ging. Vom jeweiligen Meldeamt wurde meist eine Liste aller über 18-jährigen Einwohner auf einem Datenträger zwecks Überprüfungsarbeiten erbeten. Oft vertraten die Gemeinden zunächst die Auffassung, dass nach § 16 der Meldedaten-Übermittlungsverordnung dem Südwestrundfunk lediglich die aus Anlass der An- oder Abmeldung eines Einwohners anfallenden Daten übermittelt werden dürfen.

Hier war jedoch ergänzend darauf hinzuweisen, dass der Südwestrundfunk als sonstige öffentliche Stelle nach § 31 MG bei der Auskunftserteilung privilegiert ist. Nach dieser Vorschrift darf die Meldebehörde aus dem Melderegister bestimmte Daten (auch im Rahmen einer Gruppenauskunft) übermitteln, wenn dies zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Wenn die Rundfunkanstalt in Schwerpunktbereichen, die beispielsweise altersmäßig oder nach Wohnbereichen (Stadtteilen) abzugrenzen sind, von ihrer nach dem Staatsvertrag bestehenden Befugnis zur Ermittlung unbekannter Gebührenpflichtiger Gebrauch macht, können hierfür Adressdaten aus dem Melderegister übermittelt werden. Diese Rechtsauffassung wurde durch den Verwaltungsgerichtshof Mannheim für Baden-Württemberg (Urteil vom 15. November 1994 – I S 310/94 –) ausdrücklich bestätigt.

In diesem Zusammenhang hat der LfD mit dem Datenschutzbeauftragten des Südwestrundfunks Kontakt aufgenommen mit dem Ziel einer gemeinsamen Position hinsichtlich der Weitergabe von Einwohnermeldedaten an Rundfunkgebührenbeauftragte. Es besteht Einvernehmen darüber, dass beispielsweise Anträge auf Übermittlung der Einwohnerdaten aller über 18-Jährigen – auch im Lichte des vorgenannten Urteils – durch die Regelung in § 31 MG nicht gedeckt sind. Anderenfalls würde nämlich auf Seiten des Südwestrundfunks im Laufe der Zeit ein entsprechender Gesamtbestand, sozusagen ein zweites Melderegister aller über 18-Jährigen, entstehen. Ein solches Gebilde ist indessen weder staatsvertraglich noch melderechtlich vorgesehen. Die Gebührenbeauftragten haben daher ihre Anfragen in schriftlicher Form z. B. altersgruppenmäßig (u. U. auf die 18- bis 25-Jährigen) zu begrenzen und – etwa durch statistisch belegte Aussagen – substantiiert und schlüssig darzulegen, warum sie gerade diese Meldedaten benötigen. Erst dann wird die Meldebehörde nämlich in die Lage versetzt, aufgrund der vorgetragenen Gesichtspunkte ihre Ermessensentscheidung nach § 31 MG treffen zu können.

Im Übrigen sind auch schutzwürdige Interessen einzelner Einwohnerinnen und Einwohner zu berücksichtigen. Fälle mit Auskunftssperre sind zwar nicht generell von der Übermittlung ausgeschlossen; hier sind die berechtigten Interessen der Betroffenen aber besonders sorgfältig zu prüfen.

Der Datenschutzbeauftragte des Südwestrundfunks hat die Gebührenbeauftragten inzwischen entsprechend informiert.

4.3 Datenaustausch mit kirchlichen Institutionen

Im Berichtszeitraum wurde verschiedentlich angefragt, wie oder wo der melderechtliche Datenaustausch mit kirchlichen Institutionen (s. auch Tz. 23.2) geregelt ist. Allgemein ist die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften in § 15 LDSG geregelt, wonach die Vorschriften der Datenübermittlung an öffentliche Stellen entsprechend zur Anwendung kommen, sofern sichergestellt ist, dass bei der empfangenden Stelle der Datenschutz gewährleistet ist. Nach Feststellung des rheinland-pfälzischen Innenministeriums haben die Evangelische Kirche in Hessen und Nassau, die Evangelische Kirche der Pfalz, die Evangelische Kirche im Rheinland, die Römisch-Katholische Kirche, die Alt-Katholische Kirche, die Freie Religionsgemeinschaft Alzey und die Freireligiöse Landesgemeinschaft Rheinland-Pfalz ausreichende Datenschutzmaßnahmen getroffen.

Eine Spezialregelung findet sich in § 32 MG. Danach darf die Meldebehörde einer öffentlich-rechtlichen Religionsgesellschaft zur Erfüllung ihrer Aufgaben bestimmte Daten ihrer Mitglieder und – nach Absatz 2 vorgenannter Bestimmung – von Familienangehörigen der Mitglieder, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgesellschaft angehören, übermitteln. Die Übermittlung der in § 32 Abs. 2 MG genannten Daten von Familienangehörigen ist nur zulässig, wenn die Betroffenen der Datenübermittlung nicht widersprochen haben. Der Widerspruch kann durch einfache Erklärung gegenüber der Meldebehörde erfolgen. Haben Betroffene ihr Widerspruchsrecht ausgeübt, dürfen nur solche Angaben mitgeteilt werden, die für Zwecke der Steuererhebung durch die jeweilige öffentlich-rechtliche Religionsgesellschaft erforderlich sind.

Des Weiteren ist darauf hinzuweisen, dass es Fälle gibt, in denen öffentlich-rechtliche Religionsgesellschaften über ihre innerkirchlichen Aufgaben hinaus „weltliche“ öffentliche Aufgaben wahrnehmen, die dem staatlich geordneten Bereich zuzurechnen sind. Dies gilt z. B. für das dem öffentlichen Recht zugehörende Privatschul-, Krankenhaus- und Friedhofswesen. Üben Religionsgesellschaften, die Körperschaften des öffentlichen Rechts sind, aufgrund staatlichen Rechts in solchen Fällen öffentliche Gewalt aus und umfasst der Kreis der von diesen Aktivitäten berührten Personen auch Nichtmitglieder dieser Religionsgesellschaften, so werden sie insoweit als Behörden tätig mit der Folge, dass ihnen Meldedaten übermittelt werden dürfen.

Darüber hinaus sind auch Lebenssachverhalte denkbar – z. B. auf dem Gebiet der sozialen Betreuung bestimmter Bevölkerungsgruppen wie jugendlicher, alter und behinderter Menschen –, in denen die Kirchen ebenso wie andere caritative Verbände oder Einrichtungen tätig werden. Auch hier können Datenbedürfnisse entstehen, die Nichtmitglieder betreffen. Dabei dürfen nach allgemeiner Auffassung die öffentlich-rechtlichen Religionsgesellschaften nicht schlechter gestellt werden als andere private Einrichtungen (z. B. Wohlfahrtsverbände, caritative Einrichtungen). Sofern dafür ein öffentliches Interesse anerkannt wird und die schutzwürdigen Interessen der Betroffenen gewahrt bleiben, dürfen ihnen deshalb Meldedaten zweckgebunden zur Verfügung gestellt werden.

4.4 Meldedatenübermittlung für Zwecke der Krebsvorsorge durch Mammographie-Screening

Der Bundesausschuss der Ärzte und Krankenkassen hat am 1. Dezember 2003 beschlossen, im Rahmen der Krebsfrüherkennungsrichtlinien die Früherkennung von Brustkrebs durch ein Mammographie-Screening zu ergänzen. Im Zuge einer neuen ärztlichen Leistung soll jede Frau, unabhängig davon, ob sie gesetzlich oder privat oder nicht krankenversichert ist, ab dem Alter von fünfzig Jahren bis zum Ende des siebzigsten Lebensjahres in Abstand von zwei Jahren schriftlich zu einer Untersuchung auf freiwilliger Basis eingeladen werden. Für die Einladung sollen Daten der Melderegister verwendet werden.

Die Konferenz der Gesundheitsminister hat auf ihrer 77. Sitzung Anfang 2004 den Beschluss gefasst, dass die Länder bereit sind, sich den mit der Einführung des Mammographie-Screenings verbundenen Aufgaben zu stellen. Damit verbunden sind Gesetzesanpassungen im Hinblick auf ein einheitliches bevölkerungsbezogenes System der Einladungen für die Früherkennung von Brustkrebs. Im Mai 2004 hat in der Dienststelle des LfD eine Besprechung über Einladungen für das flächendeckende Mammographie-Screening unter Beteiligung des Gesundheitsministeriums, der Kassenärztlichen Vereinigung Rheinhessen und des Innenministeriums stattgefunden. Der LfD hat in diesem Zusammenhang nochmals auf die Probleme hingewiesen, die im Bereich des Melderechts vorhanden sind, und auch die Frage der bislang ungeklärten Zuständigkeit der vorgesehenen zentralen Stelle, die das Einladungsverfahren durchführen soll, angesprochen.

Nunmehr soll im Rahmen der Novellierung des Melderechts die Meldedatenübermittlungsverordnung um eine Vorschrift ergänzt werden, die es der zentralen Stelle erlaubt, zu den jeweiligen Einladungsterminen die entsprechende Gruppenauskunft hinsichtlich der 50- bis 70-jährigen Frauen zu erhalten. Das Gesundheitsministerium wird prüfen, ob auf dem Verordnungswege die Zuständigkeit der zentralen Stelle, die wohl bei der Kassenärztlichen Vereinigung angesiedelt sein wird, begründet werden kann. Eine Lösung steht insofern noch aus.

4.5 Zugriff der „Arbeitsgemeinschaft Job-Center“ auf das Melderegister einer Stadt

In den 30 rheinland-pfälzischen Arbeitsgemeinschaften, die im Zuge der Umsetzung von „Hartz IV“ gebildet wurden, betreuen Kommunen und Arbeitsagenturen – also sowohl städtische Bedienstete als auch Mitarbeiter der Bundesagentur für Arbeit – gemeinsam die Empfänger von Arbeitslosengeld II (vgl. hierzu insbesondere Tz. 11.1).

Zur Frage, ob es zulässig war, für die Arbeitsgemeinschaft einen Direktzugriff auf die im Melderegister der Stadt gespeicherten Daten einzurichten, wurde aus der Sicht des Datenschutzes auf Folgendes hingewiesen:

Gemäß § 31 Abs. 1 MG dürfen Behörden oder sonstigen öffentlichen Stellen die in dieser Vorschrift genannten Daten übermittelt werden, soweit dies zur Aufgabenerfüllung der empfangenden Stelle erforderlich ist. Die Übermittlung personenbezogener Daten ist im Rahmen eines automatisierten Abrufverfahrens möglich, wenn innerbehördlich eine Dienstanweisung nach § 31 Abs. 1 MG i. V. m. § 7 Abs. 5 LDSG in Kraft gesetzt worden ist. Eine solche Dienstanweisung für den automatisierten Abruf von Meldedaten innerhalb der Stadtverwaltung war im vorliegenden Fall erlassen worden.

Wenn auch der Status der „Arbeitsgemeinschaft Job-Center“ zum Zeitpunkt der Anfrage nicht eindeutig geklärt war, so stand dennoch zumindest außer Frage, dass es sich hierbei um eine öffentliche Stelle handelt und insoweit die Befugnis zur Übermittlung von Meldedaten nach Maßgabe des § 31 MG gegeben ist.

Was die Möglichkeit des automatisierten Abrufs anbelangt, so hatte eine entsprechende Kontaktaufnahme mit dem Ministerium des Innern und für Sport ergeben, dass man es dort für vertretbar hielt, die Arbeitsgemeinschaft bis zu einer endgültigen Klärung für einen Übergangszeitraum der Kommune zuzuordnen. Diese Auffassung wurde vom LfD geteilt, vorbehaltlich einer entsprechenden Anpassung des Abrufverfahrens im Hinblick auf den geplanten Erlass einer Informationssystemabrufverordnung, in der dann die Einzelheiten des Abrufs aus dem Gesamtbestand der Einwohner in Rheinland-Pfalz zu regeln sind. Diese Verordnung befindet sich gegenwärtig in der Ressortabstimmung (vgl. Tz. 4.2).

5. Polizeibereich

5.1 Neue Eingriffsbefugnisse im Polizeirecht

Seit mehreren Jahren wird die Diskussion geführt, ob es erforderlich ist, in die Polizeigesetze zu Zwecken der Gefahrenabwehr, insbesondere auch der Verhütung von Straftaten, neue Befugnisse einzuführen, die – zum Teil – bislang auf den Bereich der Strafverfolgung beschränkt oder die noch gar nicht zulässig waren. Es handelt sich dabei insbesondere um folgende Befugnisse:

- Telefonabhörmaßnahmen, unter Einschluss der Feststellung des Standorts von Mobiltelefonen und von sonstigen Verbindungsdaten;
- das Abhören von Gesprächen in Geschäfts- und Wohnräumen (letzteres wird auch als „Großer Lauschangriff“ bezeichnet);
- die Videobeobachtung in privaten und öffentlich zugänglichen Räumen;
- den Einsatz von Gesichtserkennungssystemen;
- den Einsatz von Kfz-Kennzeichenerfassungs- und abgleichsystemen;
- die anlasslose Personenkontrolle (gelegentlich auch als „Schleierfahndung“ bezeichnet).

Sowohl Telefonabhör- wie akustische Wohnraumüberwachungsmaßnahmen waren bislang bereits im Strafverfolgungsbereich zulässig. Der Unterschied zu präventiv-polizeilichen Befugnissen besteht primär darin, dass im Bereich der Strafverfolgung Voraussetzung des Einsatzes dieser Mittel das Vorliegen eines Anfangsverdachtes ist. Es müssen also tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist oder dass sie konkret geplant wird, weil erst dann vom Vorliegen eines strafbaren Versuchs ausgegangen werden kann.

Die polizeirechtlichen Regelungen zur akustischen Wohnraumüberwachung verlangen dagegen das Vorliegen einer dringenden Gefahr. Es müssen Tatsachen vorliegen, die darauf hindeuten, dass bestimmte Personen besonders schwerwiegende Straftaten begehen werden. Welcher Gewissheitsgrad hier vorliegen muss, ist nicht völlig klar. Möglicherweise müssen nur Planungen zur Begehung von Straftaten befürchtet bzw. erwartet werden. Unter Umständen reicht es aus, dass bestimmte Tatsachen eine gewisse Wahrscheinlichkeit begründen, dass solche Planungen erfolgen. Mit anderen Worten: die Straftatenbekämpfung kann in das Vorfeld des strafrechtlichen Anfangsverdachts verlegt werden.

Die Fachleute der Polizei vertreten ganz überwiegend, dass eine solche Erweiterung der Eingriffsmöglichkeiten angesichts heutiger Verhältnisse nötig sei, wobei regelmäßig die maßgeblichen Stichworte „organisiertes Verbrechen“, „grenzüberschreitende Kriminalität“ und „internationaler Terrorismus“ genannt werden. Wenn sich die übergroße Mehrheit der politisch Verantwortlichen davon überzeugen lässt und die Gefährdungslage so sieht, dann kann der Datenschutzbeauftragte weder aufgrund überlegener Sach- und Fachkenntnis, die er in Bezug auf die Kriminalitätslage naturgemäß nicht besitzt, noch aufgrund sonstiger Gesichtspunkte dieser Einschätzung widersprechen. Seine Rolle kann nur darin bestehen, bei den für nötig befundenen staatlichen Reaktionen zur Bekämpfung der genannten Gefahren auf die Beachtung der verfassungsrechtlichen Standards hinzuwirken.

In diesem Sinn ist der LfD wiederholt im Gesetzgebungsverfahren der diesbezüglichen POG-Novellierung tätig geworden. Er hat sich vielfach sowohl im Vorfeld des Gesetzgebungsverfahrens gegenüber dem ISM, dann auch im Innenausschuss des Landtags und gegenüber den Fraktionen geäußert und ausführlich Stellung genommen. Der Landtag hat sich die Entscheidung gewiss nicht leicht gemacht; nach ausführlichen Beratungen und einer Anhörung auch externer Experten hat er entschieden. Nach der Einschätzung des LfD ist das Ergebnis durchaus auch aus datenschutzrechtlicher Sicht akzeptabel, wenn auch gewisse Vorbehalte an eher marginalen Punkten fortbestehen.

Hervorzuheben ist, dass nach den nunmehr im POG vorhandenen Regelungen für die Telefonabhörmaßnahmen wie für den „Großen Lauschangriff“ ein absolutes Verbot des Eindringens in die Sphäre besonderer Berufs- und Vertrauensverhältnisse normiert worden ist.

Nach dem Urteil des Bundesverfassungsgerichts zum strafprozessualen „Großen Lauschangriff“ (vom 3. März 2004, Az.: 1 BvR 2378/98) wurde die entsprechende Bestimmung des POG dahingehend ergänzt, dass auch das Eindringen in höchstpersönliche Vertrauensverhältnisse auszuschließen ist (§ 29 Abs. 3 bis 5 POG, GVBl. 1993, S. 595, zuletzt geändert durch Gesetz vom 25. Juli 2005, GVBl. 2005, S. 320).

Es besteht eine Unterrichtungspflicht gegenüber den Betroffenen, sobald dies ohne Gefährdung der polizeilichen Ziele möglich ist. Außerdem ist Voraussetzung solcher Maßnahmen, dass ein Richter entschieden hat. Zur Berichts- und Prüfpflicht hinsichtlich des Fortbestehens dieser Regelungen s. unten Tz. 5.2.

Auch vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts zu den Telefonabhörmöglichkeiten nach dem niedersächsischen Sicherheits- und Ordnungsgesetz (Urteil vom 27. Juli 2005, Az. 1 BvR 668/04) ergibt sich kein unmittelbar zwingender Handlungsbedarf zur Änderung der entsprechenden rheinland-pfälzischen Regelung. Die in Niedersachsen aufgehobene Norm hat im rheinland-pfälzischen Gesetz keine unmittelbare Entsprechung, und die der rheinland-pfälzischen Norm parallele Regelung des niedersächsischen Gesetzes wurde vom Verfassungsgericht gerade nicht aufgehoben oder gerügt.

Ein Prüfbedarf, ob nicht weitere Folgerungen aus den genannten Verfassungsgerichtsentscheidungen zu ziehen sind, bleibt allerdings bestehen. Die Überlegungen hierzu dauern an. Festzustellen ist – dies ergibt sich aus den genannten verfassungsgerichtlichen Entscheidungen –, dass sich die Gesetzgeber allgemein in diesem Bereich hart am Rand des verfassungsrechtlich noch Zulässigen bewegen. Dies sollte zu denken geben und Anlass zu einem sehr vorsichtigen Vorgehen bei allen Erweiterungen von polizeilichen Eingriffsbefugnissen sein.

5.2 Evaluierung der besonderen neuen polizeirechtlichen Eingriffsmaßnahmen

Der im Rahmen der Novellierung des POG neu geschaffene § 100 POG sieht eine gesetzliche Berichtspflicht der Landesregierung zur Überprüfung der Normeffizienz („Evaluierung“) bestimmter polizeilicher Befugnisse vor. Gegenstand dieser Evaluierung (der Berichtszeitraum erstreckt sich über fünf Jahre) sollen die Sicht- und Anhaltekontrollen im öffentlichen Verkehrsraum, die Maßnahmen der Telekommunikationsüberwachung, der Große Lauschangriff und die Rasterfahndung sein. Zur Vorbereitung der Datenerhebungen durch die polizeilichen Einsatzkräfte wurden vom ISM erforderliche und angemessene Messkriterien, der Umfang der zu erhebenden Daten und die Erarbeitung von Richtlinien festgelegt. In diese Überlegungen wurde der LfD frühzeitig eingebunden, so dass seine Empfehlungen, die die datenschutzrechtliche Zielsetzung der Überprüfungsmaßnahmen zum Ausgangspunkt hatten, in die Gestaltung der Erfassungsformblätter einfließen konnten.

Unabhängig von diesen Evaluierungsmaßnahmen hat die Polizei gem. § 29 Abs. 7 Satz 1 POG eine jährliche Unterrichtungspflicht über den erfolgten verdeckten Einsatz technischer Mittel. In ihrem entsprechenden Bericht an den Landtag wird ausgeführt, dass wegen der geringen Zahl der im Berichtszeitraum zur Prävention durchgeführten Überwachungsmaßnahmen von einem äußerst verantwortungsbewussten Einsatz dieses Mittels ausgegangen werden könne (vgl. LT-Drs. 14/4292 vom 29. Juni 2005). Angesichts der dort genannten geringen Zahlen kann dieser Einschätzung nicht widersprochen werden. Ob sich diese Entwicklung fortsetzt, wird der nächste Erfahrungsbericht, der Mitte 2006 zu erwarten ist, zeigen.

5.3 Örtliche Feststellungen bei Polizeidienststellen

Der LfD hat sich im Berichtszeitraum wiederum darum bemüht, durch regelmäßige Vor-Ort-Kontrollen die polizeiliche Datenverarbeitung zu überprüfen. Dies kann selbstverständlich nur stichprobenweise und nicht flächendeckend erfolgen. Im Berichtszeitraum erfolgten in den fünf Präsidialbereichen bei neun Polizeidienststellen (inklusive Landeskriminalamt) örtliche Feststellungen. Beanstandungen wurden hierbei nicht ausgesprochen.

Im Zusammenwirken mit dem Innenministerium ist es allerdings regelmäßig gelungen, erkannte Schwachpunkte zu korrigieren und auch durch generelle Anweisungen im gesamten Land Verbesserungen zu erreichen. Dies gilt beispielsweise für die Aktualisierung der polizeilichen Erkenntnisse durch ein Verfahren, das die Unterrichtung der Polizei über das Ergebnis der staatsanwaltlichen Tätigkeiten sicherstellt. Ein anderes Beispiel ist die generelle Regelung von zentralen Auswertungen des polizeilichen Vorgangsbearbeitungssystems POLADIS.

Einen wesentlichen Bestandteil der im Berichtszeitraum geführten Beratungs- bzw. Informationsgespräche mit der Zentralstelle für Polizeitechnik, dem Landesbetrieb Daten und Information, dem Landeskriminalamt und dem Ministerium des Innern und für Sport bildeten die datenschutzrechtlichen Anforderungen an die im Rahmen der Fußballweltmeisterschaft 2006 von der Polizei beabsichtigten Überwachungsmaßnahmen (Datenerhebungen durch Aufzeichnungssysteme, Datenabgleiche, Akkreditierungsverfahren).

Trotz einer überwiegend positiven Bilanz bestand dennoch bei einigen örtlichen Feststellungen Anlass, Verbesserungsvorschläge aus datenschutzrechtlicher Sicht zu formulieren. In allen Fällen konnte Konsens mit dem Innenministerium erzielt werden.

Im Einzelnen sah der LfD bei folgenden Themen Handlungsbedarf:

- Einsicht in das Pass- und Personalausweisregister zur Ermittlung von Fahrzeugführern im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten darf nur von den Bediensteten genommen werden, die hierfür vom Behördenleiter besonders ermächtigt worden sind. Nach §§ 22 Abs. 3 Passgesetz, 2 b Abs. 3 Personalausweisgesetz sind Anschrift des Betroffenen, Anlass der Übermittlung und Vernichtungsfristen aktenkundig zu machen. Auch in diesem Berichtszeitraum fehlten bei einigen Dienststellen entweder die erforderlichen Aufzeichnungen über Einsichtnahmen in die Lichtbildkartei des Pass- und Ausweisregisters zur Verfolgung von Verkehrsordnungswidrigkeiten, die schriftliche Dokumentation der für die Einsichtnahme Ermächtigten oder die Anzahl der Ermächtigten war unangemessen groß (bis zu allen Beamten). Den Empfehlungen des LfD, die Zahl der Ermächtigungen hinsichtlich der Erforderlichkeit zu prüfen und die Dokumentation der Einsichtnahme zu überwachen, wurde entsprochen.
- Im Berichtszeitraum fanden zahlreiche Beratungen mit dem ISM zu ergänzenden Anwendungen und Errichtungsanordnungen/Verfahrensbeschreibungen des 2003 eingeführten Vorgangsbearbeitungssystems POLADIS.net statt. Die bereits im 19. Tätigkeitsbericht problematisierten dienststellenspezifischen Löschmodalitäten (Verfügbarkeit der Vorgangsverwaltungsdaten bis maximal zehn Jahre nach Ermittlungsabschluss) von POLADIS.net hatte der LfD in der Folge zum Gegenstand örtlicher Feststellungen bei verschiedenen Polizeidienststellen gemacht. Die bereits bei Abstimmung der Generalerrichtungsanordnung für die Datei POLADIS.net gegenüber dem Innenministerium dargelegten Bedenken hinsichtlich der langen Speicherdauer von Verwaltungsdaten, haben sich dabei konkretisiert. Selbst wenn, wie in einem Fall festgestellt, die Vorgangssachbearbeitungsdaten aufgrund eines Verfahrenshindernisses (es liegt überhaupt keine Straftat vor) unverzüglich nach Einstellung des Verfahrens gelöscht werden, sind die Vorgangsverwaltungsdaten mindestens noch ein Jahr nach Löschung der Sachbearbeitungsdaten verfügbar. Bei dem in Rede stehenden Fall war der nach Abschluss des Verfahrens unzutreffende Status „Beschuldigte“ noch ein Jahr nach der Klarstellung recherchierbar. Im zitierten Einzelfall war diese Verfahrensweise aus datenschutzrechtlicher Sicht nicht bedenklich, weil dem Erfordernis aus § 19 Abs. 1 Satz 3 LDSG durch einen den Sachverhalt richtig stellenden Eintrag in dem Datenfeld „Meldungsdaten – Inhalt der Meldung“ Rechnung getragen wurde, der als Teil der Vorgangsverwaltungsdaten bis zur Komplettlöschung verfügbar ist. Generell ist, wie beim ISM vom LfD angeregt, die Speicherdauer von Vorgangsverwaltungsdaten zu überdenken.

5.4 Speicherung personengebundener Hinweise in POLIS/INPOL

Strategische Fortentwicklungen der elektronischen Auskunfts- und Informationssysteme (POLIS/INPOL.net) führten zu einer Erweiterung des Datenfeldes PHW (personengebundene Hinweise) vom ursprünglichen Zweck der Eigensicherung von Polizeibeamten hin zu einer stärkeren Gewichtung ermittlungsrelevanter Hinweise zur Kriminalitätsbekämpfung. Damit einhergehend war eine deutliche Zunahme der Vergabe von personengebundenen Hinweisen zu beobachten. Im Rahmen örtlicher Feststellungen und durch eine systematische Stichprobenauswertung polizeilicher Akten stellte der LfD fest, dass nicht bei allen Polizeidienststellen die Vergabe der PHW „geisteskrank“, „gewalttätig“ und „Sexualtäter“ am Erforderlichkeitsgrundsatz orientiert war.

Beim PHW „Ansteckungsgefahr“ sowie beim Merkmal „geisteskrank“ wurden in einigen Fällen die formellen Anforderungen nicht erfüllt (Hinweis auf die Quelle der Information bzw. Angabe von Urheber und Aufbewahrungsort des maßgeblichen Gutachtens). Die diesbezüglichen Erörterungen mit dem ISM auch im Hinblick auf die Ausgestaltung der Bundesdatei „INPOL-neu“ dauern an.

5.5 Neue Techniken

5.5.1 Polizeiliches Fachinformationsnetz EXTRAPOL

Im 19. Tätigkeitbericht hatte der LfD unter Tz. 5.21 über das Fachinformationsnetz der Polizeien EXTRAPOL berichtet. Das Verfahren wurde zwischenzeitlich in den Wirkbetrieb überführt. Gleichzeitig wurden die Zuständigkeiten neu geordnet; in diesem Zusammenhang hat Rheinland-Pfalz einen Teil der EXTRAPOL-Verantwortung abgegeben. Die inhaltliche Gestaltung und Betreuung des Verfahrens liegt nunmehr in Händen einer Fachredaktion, den Vorsitz führt hier das Landeskriminalamt Hessen.

EXTRAPOL ist grundsätzlich als dezentrales Netz konzipiert, der technische Betrieb zweier Komponenten – des Redaktionssystems und der eigentlichen Informationsplattform – erfolgt allerdings weiterhin zentral im Weg der Auftragsdatenverarbeitung durch den Landesbetrieb Daten und Information.

Konzipiert wurde EXTRAPOL ursprünglich als Plattform für polizeiliche Fachinformationen (Dienstvorschriften, Rechtsgrundlagen, Fachdokumentationen etc.). Bereits 2003 wurden allerdings Meldungen zu überregional bedeutsamen Ereignissen und Vorkommnissen aufgenommen. Ein weiterer Schritt hin zur Aufnahme fallbezogener Informationen ist mit der Einstellung des Bundeskriminalblatts des BKA erfolgt. Die Planungen zur weiteren Entwicklung von EXTRAPOL gehen dahin, die Plattform für den direkten Informationsaustausch der Polizeien untereinander auszubauen.

Im Zusammenhang mit dem Ausbau der Funktionalität wurde ein Berechtigungsmodell eingeführt, das die Bildung geschlossener Benutzergruppen ermöglicht. Die eingesetzte Lösung ist grundsätzlich geeignet, auch feiner abgestufte Berechtigungen zu verwalten, tut dies gegenwärtig jedoch nicht. Zudem ist das Berechtigungskonzept derzeit nur für Teilbereiche realisiert. Protokollierungsfunktionen, die über die serverseitige Erfassung der Inhalte und der abrufenden Stelle hinausgehen, existieren außerhalb des Redaktionssystems bislang nicht; Abfragen oder der Zugriff auf einzelne Informationen sind damit benutzerbezogen nicht nachvollziehbar.

Personenbezogene Daten werden in EXTRAPOL gegenwärtig nur in Randbereichen verarbeitet. Mit Blick auf die Weiterentwicklung des Verfahrens sind aus Sicht des LfD parallel hierzu die Sicherheits- und Datenschutzmechanismen nachzuführen, jedenfalls dann, wenn – wie vorgesehen – ein weiterer Ausbau zu einer umfassenden Informations- und Kommunikationsplattform erfolgen sollte.

5.5.2 Gesichtserkennungssysteme

Die Polizei Rheinland-Pfalz erprobt derzeit eine Lösung zur automatischen Gesichtserkennung in Videoaufnahmen („FaceSnap“). Es handelt sich dabei um eine Kombination aus Kamera, digitalem Videorecorder und biometrischer Gesichtserkennungssoftware („FaceRecorder“). Die Lösung ist portabel und wird bei Observationen durch das Mobile Einsatzkommando des LKA eingesetzt. Die FaceSnap-Software wertet Videoaufnahmen aus, findet und extrahiert daraus selbständig Gesichtsbilder und speichert diese in einer internen Datenbank. Falls mehr als eine Person gleichzeitig im Bild ist, werden auch mehrere Gesichter erfasst. Aufnahmen, die keine Gesichter enthalten, verwirft das System. Über eine weitere Komponente ist ein nachträglicher Abgleich der extrahierten Bilder mit Vergleichsaufnahmen möglich.

Das System dient der erleichterten Auswertung von Videoaufzeichnungen aus Observationen und erlaubt zur Personenerkennung einen automatischen Abgleich mit einer beschränkten Zahl von Vergleichsaufnahmen gleichzeitig. Nach Abschluss einer Maßnahme werden die Bilder auf CD-ROM gesichert und im FaceSnap-System gelöscht.

Über Erweiterungen sind die Anbindung an eine externe Bilddatenbank und der Online-Abgleich in Echtzeit während der Videoaufzeichnung möglich („FaceServer“). In dieser Form wird die Lösung u. a. für die Zutrittsüberwachung an Flughäfen und zur Überwachung bestehender Hausverbote in Spielbanken eingesetzt. Über eine weitere Ergänzung („FaceTrack“) ist es möglich, auch in großflächigen Überwachungsaufnahmen Gesichter automatisch zu detektieren, heranzuzoomen und herauszufiltern.

In der gegenwärtigen Form wird die FaceSnap-Lösung isoliert für einzelne Observationsmaßnahmen durch das MEK, von einem eng begrenzten Personenkreis und unter festgelegten Bedingungen genutzt. In diesem Zusammenhang begegnet sie dabei keinen datenschutzrechtlichen Bedenken.

Bei vielen aktuellen Videolösungen handelt es sich um „intelligente Kameras“, ausgestattet mit Prozessoreinheit, Massenspeicher, Netzwerkanschluss und Betriebssystem – letztlich videotaugliche PCs. Dies gilt auch für die FaceSnap-Lösung. Im Fall einer Erweiterung des Einsatzspektrums und insbesondere bei einer Einbindung in vorhandene IT-Strukturen der Polizei bedarf es aus Sicht des LfD einer Anpassung der Datenschutz- und Datensicherheitsfunktionen, die eine angemessene Zugriffs- und Verarbeitungskontrolle nach § 9 Abs. 2 LDSG sicherstellen (z. B. Benutzerverwaltung, Protokollierung).

Als Rechtsgrundlage für den Einsatz dieses Verfahrens ist im Bereich der Strafverfolgung § 100 c Abs. 1 StPO, im Bereich der Gefahrenabwehr § 37 Abs. 3 POG zu beachten. Diese Regelungen beschränken die Einsatzmöglichkeiten. Der LfD wird den praktischen Einsatz weiterhin aufmerksam beobachten.

5.5.3 Digitalisierte Fingerabdruckverarbeitung

Die Polizei Rheinland-Pfalz erprobt derzeit im Rahmen eines Pilotprojekts unter der Leitung des BKA den Einsatz von Lösungen, mit denen eine mobile Identifizierung anhand digital aufgenommener Fingerabdrücke möglich ist („Fast Ident"). Das Verfahren soll bei der WM 2006 unter anderem bei der Besucherkontrolle, bei Kontrollen an den Landesgrenzen sowie bei der Überprüfung von festgenommenen Personen eingesetzt werden.

Die Geräte sind mit einem Fingerabdruckscanner ausgestattet; die gescannten Abdrücke werden gegen einen im Gerät gespeicherten Teildatenbestand aus dem AFIS-System des Bundeskriminalamts geprüft. Dieser wird manuell aktualisiert, indem in regelmäßigen Abständen der jeweils aktuelle Stand aufgespielt wird. Die digital abgenommenen Fingerabdrücke werden nicht dauerhaft im Gerät gespeichert. In einem zweiten Schritt ist beabsichtigt, drahtlos auf den AFIS-Gesamtbestand zuzugreifen.

Die Fast Ident-Lösung bietet gegenwärtig nur eine beschränkte Verlässlichkeit der Identifizierung. Bei Tests wurde eine Treffergenauigkeit von ca. 56 % erreicht. Es ist kritisch zu fragen, ob eine derart geringe Genauigkeit den Einsatz eines solchen Systems überhaupt erlaubt. Auch bei einer Erhöhung der Treffergenauigkeit dürfen aus Sicht des LfD allein auf der Grundlage eines angezeigten „Treffers" jedenfalls keine Eingriffsmaßnahmen getroffen, sondern es müssen ergänzende Identifizierungsmaßnahmen ergriffen werden. Er hat daher empfohlen, in einer Dienstanweisung festzulegen, welche polizeilichen Maßnahmen bei welcher Trefferwahrscheinlichkeit zur Anwendung kommen sollen, einen angemessenen Zeitrahmen für die Aktualisierung der Vergleichsdaten vorzusehen und nach Abschluss der Pilotphase das Löschen von Protokolldaten sicher zu stellen.

Weitergehende Planungen der Polizei sehen vor, die erkennungsdienstliche Behandlung allgemein auf die digitale Fingerabdruckverarbeitung umzustellen. Nicht zuletzt mit Blick auf die Fußballweltmeisterschaft 2006 sollen die Präsidien bis Mitte des nächsten Jahres mit der hierzu erforderlichen Infrastruktur ausgestattet werden. Parallel dazu soll eine gesonderte Landesdatei eingerichtet werden, die neben der Speicherung digitalisierter Finger- und Handflächenabdrücke den Abgleich von Fingerabdruckspuren und die Übermittlung digitalisierten ED-Materials an die AFIS-Datenbank des BKA unterstützt.

Der LfD wurde über die Planungen der Polizei in diesem Bereich unterrichtet und wird die weitere Entwicklung verfolgen.

5.5.4 Digitalisierte Unterstützung von komplexen Ermittlungsverfahren

Im 18. Tätigkeitsbericht hatte der LfD unter der Tz. 21.2.3 über ein Verfahren berichtet, das die zusammenhängende Aufbereitung und Darstellung polizeilicher Ermittlungsergebnisse ermöglicht. Die Lösung wurde zwischenzeitlich weiter entwickelt und wird gegenwärtig unter der Bezeichnung KRISTAL (Kriminalpolizeiliches Recherche- und Informationssystem; Täterorientierte Auswertung/Analyse und Lagedarstellung) in bestimmten Ermittlungsbereichen erprobt.

Die Lösung dient der Auswertung und Darstellung der Zusammenhänge von Daten aus unterschiedlichen Fachanwendungen der Polizei (POLADIS, ATIS, POLIS etc.) sowie aus Verfahren anderer Verwaltungsbereiche (z. B. EWOIS). Anstelle einer separaten Abfrage im jeweiligen Verfahren werden vorselektierte Daten automatisiert übergeben und die Ergebnisse in KRISTAL übernommen. Letztlich fasst KRISTAL ermittlungsrelevante Daten aus unterschiedlichen Anwendungen zusammen und bietet die Möglichkeit der nach Zeit bzw. Häufigkeit ausgerichteten Visualisierung von Beziehungen z. B. zwischen Personen, Objekten und Vorkommnissen. Für die sich daraus ergebenden Fragen der Zugriffskontrolle, der Nachvollziehbarkeit der Nutzung und der Gewährleistung notwendiger Datenlöschungen sollten aus Sicht des LfD vor einer flächendeckenden Einführung praktische Erfahrungen aus einem Testbetrieb in die datenschutzrechtliche Bewertung einfließen.

Für das Verfahren wurden eine Vorabkontrolle nach § 9 Abs. 5 LDSG durchgeführt und Verarbeitungsregeln festgelegt. Aus Sicht des LfD bestanden damit keine Bedenken gegen die Aufnahme des Pilotbetriebs; er wird den weiteren Einsatz des Verfahrens aufmerksam begleiten.

5.5.5 RIVAR

Eine der zentralen Anwendungen des RIVAR-Verfahrens ist die polizeiliche Vorgangsverwaltung POLADIS (vgl. 18. Tb., Tz. 5.2; 19. Tb., Tz. 5.11.1). Das Verfahren wird landesweit bei allen Polizeidienststellen eingesetzt; die Datenhaltung basiert derzeit auf 126 getrennten Datenbanksystemen. Mit Blick auf den damit verbundenen Administrations- und Betreuungsaufwand werden seitens der Polizei Überlegungen angestellt, die Datenhaltung ganz oder teilweise zu zentralisieren. Zur Klärung der Vor- und Nachteile derartiger Lösungen und zur Prüfung möglicher Realisierungsalternativen ist eine Machbarkeitsstudie vorgesehen.

Der LfD wurde frühzeitig in die Zentralisierungsüberlegungen eingebunden. In diesem Zusammenhang hat er auf die Notwendigkeit hingewiesen, die mit einer Konsolidierung der Datenhaltung verbundenen erleichterten Zugriffs- und Auswertungsmöglichkeiten durch entsprechende Protokollierungsmechanismen und Berechtigungskonzepte zu kompensieren. Der in der Vergangenheit in der datenschutzrechtlichen Bewertung häufig bedeutsamen Unterscheidung zwischen zentraler und dezentraler Datenhal-

tung kommt nach Auffassung des LfD im Zeitalter vernetzter Systeme und verteilter Anwendungen zunehmend geringere Bedeutung zu. Organisationsweite Administrationslösungen ermöglichen, wenngleich mit erhöhtem Aufwand, auch bei dezentralen Strukturen zentrale Zugriffe und Recherchemöglichkeiten. Datenschutzrechtliche Vorteile ergäben sich bei einer Konsolidierung der POLADIS-Datenhaltung hinsichtlich der Auswertung von Protokolldaten. Da diese verbunden mit der jeweiligen Datenbank gespeichert werden, lassen sich einzelne Abrufe gegenwärtig nur mit entsprechendem Aufwand klären. Dem LfD wurde zugesagt, ihn im Rahmen der weiteren Entwicklung zu beteiligen.

Die zentrale Nutzung von Daten der dezentralen polizeilichen Vorgangsverwaltung stellt offensichtlich eine polizeiliche Notwendigkeit dar. Im Berichtszeitraum hatte der LfD zu beurteilen, ob eine solche Auswertung zu kriminalstatistischen Zwecken zulässig war; in einem anderen Fall ging es um die Suche nach einem verdächtigen Fahrzeug, das möglicherweise schon in einem anderen Zusammenhang polizeilich erfasst worden war. Der LfD hält solche Nutzungen für unvereinbar mit der gegenwärtigen Dateierrichtungsanordnung POLADIS. Er hat deshalb angeregt, für Fälle, in denen eine solche Nutzung als allgemeines polizeiliches Informationssystem unabweisbar erscheint, die Errichtungsanordnung zu ändern; selbstverständlich sind solche Nutzungen nur dann zulässig, wenn sie aufgrund von Protokollierungen nachvollziehbar sind und eine herausragende Bedeutung für die polizeiliche Aufgabenerfüllung haben.

Im Rahmen einer Kooperation zwischen Rheinland-Pfalz und dem Saarland übernimmt die Polizei des Saarlandes Fachanwendungen aus dem RIVAR-Konzept. Zunächst betrifft dies das Polizeiliche Informationssystem POLIS als Landeskomponente des INPOL-Verfahrens sowie in einem weiteren Schritt die polizeiliche Vorgangsverwaltung POLADIS. Der technische Betrieb des POLIS-Verfahrens für das Saarland obliegt dem LDI, die Verfahrensbetreuung hingegen der dortigen Polizei bzw. dem IT-Dienstleister der saarländischen Landesverwaltung.

Kernpunkt der Bewertung des LfD war in diesem Zusammenhang die Frage, ob sich aus der Nutzung der Infrastruktur des LDI datenschutzrechtliche Risiken für das POLIS-Verfahren Rheinland-Pfalz ergeben. Das Konzept des LDI sieht für den POLIS-Betrieb grundsätzlich getrennte Infrastrukturen vor. Netzseitig wird diese für POLIS-SL in einem eigenen logischen Teilnetz des rlp-Netzes angesiedelt. Die Anbindung des LKA Saarbrücken erfolgt über eine separate, verschlüsselte Leitungsverbindung; die Administration der Netz- und Krypto-Komponenten liegt in der Verantwortung des LDI. Damit steht der Zugang der Polizei des Saarlandes zum rlp-Netz und den POLIS-Datenbank- und Anwendungsservern unter der Kontrolle des LDI. Die Steuerung der Kommunikation ab dem Übergabepunkt in Saarbrücken liegt in saarländischer Hand.

Die Übernahme des POLIS-Betriebs für das Saarland durch den LDI führt damit zu keinen Beeinträchtigungen des Verfahrens in Rheinland-Pfalz. Das Konzept des LDI begegnete keinen datenschutzrechtlichen Bedenken. Für den Fall einer Übernahme weiterer RIVAR-Anwendungen ist das o. g. Betriebskonzept grundsätzlich übertragbar.

5.5.6 Digitale Videoaufzeichnungen von Polizeikontrollen

Die Realisierung der polizeilichen Planung, Streifenwagen mit Videokameras auszustatten, (vgl. 18. Tb., Tz. 5.8) ist im Berichtszeitraum vorangeschritten. Das Ende 2004 im Probebetrieb präsentierte, in einem Polizeibus installierte digitale Aufzeichnungssystem besteht aus einem Objektiv, einem Vorschaumonitor und einem Recorder mit Wechselfestplatte. Mit dem Einschalten der Fahrzeugfunkanlage wird das Videoaufzeichnungsgerät automatisiert in den „Stand-By-Betrieb“ geschaltet, beim Einschalten der Signalisierung „Stopp-Polizei“ die Aufzeichnung aktiviert und beim Ausschalten deaktiviert. Es ist jedoch auch möglich, die Aufzeichnung manuell zu starten bzw. zu beenden. Der Aufnahmevorgang kann über ein in den Sonnenschutz integriertes Display verfolgt werden. Ein rotes Blinklicht in der an der Frontscheibe montierten Kamera signalisiert die Aufzeichnung. Die Aufzeichnungskapazität des Speichermediums beträgt sechs Stunden. Daten, die älter als 24 Stunden sind, werden durch Überschreiben der jeweils ältesten gelöscht. Während der Aufzeichnung werden die Daten systemseits verschlüsselt. Den Anregungen des LfD, eine automatisierte Protokollierung (wer was wann wie genutzt hat) zu gewährleisten und den Zugriff nur auf die selbst erzeugten Daten zu gewährleisten, wurde entsprochen.

Für diese Verfahrensweise wurde im neuen POG nunmehr eine ausdrückliche Rechtsgrundlage geschaffen (§ 27 Abs. 4 POG).

Umstritten war zunächst, in welchem Umfang eine Auswertung der Aufnahmen zu Zwecken der Dienstaufsicht und zu Zwecken der eigenen Fortbildung der handelnden Beamten zulässig sein sollte. Diese Fragen wurden in einer Dienstvereinbarung mit dem Personalrat der Polizei, an deren Formulierungen auch der LfD mitgewirkt hatte, geregelt (s. 19. Tb., Tz. 5.4). Dem LfD ist nicht bekannt geworden, dass sich in der Praxis hier Probleme ergeben hätten.

5.6 Führt die Polizei eine Homosexuellen-Datenbank?

Die Polizeibehörden Bayerns, Thüringens und Nordrhein-Westfalens nutzten bei ihrer Ermittlungsarbeit laut Medienberichten eine Software, die auch Homosexuelle gesondert ausweisen kann. Bei Eingabe in die dort eingesetzten Vorgangsverwaltungsprogramme IGVP und PVP könne die sexuelle Neigung von Tätern, aber auch von Opfern und Zeugen, extra eingegeben werden, wie das Nachrichtenmagazin „Spiegel“ im Juli 2005 berichtete. Das Programm könne alle in Straf- oder Ermittlungsverfahren verwickelten Personen, also Täter, Opfer und Zeugen, mit ihrer homosexuellen Orientierung registrieren. Homosexuelle würden als Tätergruppe klassifiziert und „Aufenthaltsorte von Homosexuellen“ als potentielle Tatorte. Mit dem Kürzel „omosex“ sei es den Ermittlern dann möglich, sämtliche entsprechenden Datensätze abzurufen.

Nordrhein-Westfalen und Bayern hätten nach den Presseberichten das Stichwort „Aufenthaltsort von Homosexuellen“ inzwischen zwar sperren lassen, „Homosexuelle“ als Tätergruppe bleibe aber nach wie vor gültig.

Die Überprüfungen des LfD haben ergeben, dass für die vergleichbaren in Rheinland-Pfalz eingesetzten Vorgangsverwaltungsprogramme (insbesondere POLADIS) keine vergleichbaren Kataloge für die Charakterisierung von Tatorten oder Tatbeteiligten existieren. Eine gezielte Suche nach homosexuell orientierten Tatbeteiligten mithilfe der polizeilichen Vorgangsverwaltungsdateien ist deshalb hier nicht möglich.

5.7 „Beweissicherungs- und Festnahmeeinheiten (BFE)“ der Polizei

Im Zusammenhang mit den unten (Tz. 5.10) dargestellten Feststellungen anlässlich des Bush-Besuchs in Mainz ist der LfD auf die Tätigkeit von besonderen polizeilichen Einheiten zur Beweissicherung und Festnahme (BFE) aufmerksam geworden.

Derartige Einheiten dürften inzwischen in allen Bundesländern existieren. Sie werden hauptsächlich bei Demonstrationen oder sonstigen Großereignissen (z. B. Fußballspielen) eingesetzt, bei denen gewalttätige Auseinandersetzungen zu erwarten seien. Sie sind grundsätzlich bei der Bereitschaftspolizei angesiedelt; Untergliederungen dieser Einheiten sind Trupps oder Gruppen. Diese bestehen jeweils aus einem Führer und sechs oder zehn Mitgliedern. Ihre Dokumentationsaufgabe erfüllen sie dadurch, dass normalerweise zwei Mitglieder mit Videokameras die Einsätze filmen. Dabei soll insbesondere der Anlass des jeweiligen Eingreifens und sein Ablauf (Gewalttaten von Demonstranten, Widerstandshandlungen) dokumentiert werden.

Von besonderem datenschutzrechtlichen Belang ist dabei die Frage, ob bzw. unter welchen Voraussetzungen Wohnungsdurchsuchungen von einer solchen Einheit durchgeführt und mithilfe von Videogeräten dokumentiert werden.

Weiter ist in diesem Zusammenhang von Interesse für den Datenschutz, wie mit den entstandenen Video-Aufnahmen umgegangen wird, wer sie zur Kenntnis erhält, wie sie von wem ausgewertet und wie lange sie aufbewahrt werden. Besonders dann, wenn sich keine Strafverfahren anschließen und nicht die strafprozessualen, sondern die polizeirechtlichen Regelungen zur Anwendung kommen, besteht Klärungsbedarf.

Auch die Frage, ob und ggf. in welcher Form eine Zusammenarbeit (z. B. im Wege von Informationsübermittlungen) mit dem Verfassungsschutz besteht, ist datenschutzrechtlich bedeutsam. Der LfD bemüht sich derzeit um die Klärung dieser Fragen.

5.8 Überprüfungen von DNA-Analysen in Strafverfahren

Im Berichtszeitraum hat der LfD die Datenverarbeitung im Rahmen von DNA-Analysen beim Landeskriminalamt überprüft. Schwerpunkte waren der Umgang mit den Daten in Verfahren, bei denen keine Übereinstimmung zwischen Spur und Beschuldigtenprobe bestand (in denen der Verdächtige also durch die DNA-Analyse entlastet wurde), die Aktenhaltung der Verwaltungsvorgänge und der dabei bestehende technisch-organisatorische Datenschutz sowie Funktionalitäten der „neuen“ DNA-Verbunddatei (INPOL-Falldatei).

Datenschutzrechtlich bedenklich ist aus der Sicht des LfD die Dauer der Aufbewahrung von Proben und Informationen, die im Zusammenhang mit DNA-Analysen entstanden sind und die z. T. seit 1997 im LKA aufbewahrt werden. Dazu gehören Datenspeicherungen im DNA-Tagebuch der kriminaltechnischen Untersuchungsstelle sowie das Probenmaterial und die zugehörigen Akten (Untersuchungsanträge, Analyseprotokolle, Gutachten und verformelte Ergebnismitteilungen). Löschungen auch von Altfällen sind nach den Angaben der Mitarbeiter des LKA nicht erfolgt, wenn und soweit für die zugrunde liegenden DNA-Proben keine ausdrücklichen Vernichtungsanordnungen der Staatsanwaltschaften erlassen wurden. Dies sei nur in sehr wenigen Fällen geschehen.

Datenschutzrechtlichen Bedenken begegnet insbesondere die übermäßig lang dauernde Aufbewahrung von Daten und Proben solcher Personen, die nicht mehr Beschuldigte sind („Ausschlüsse“) sowie von „Nichtbeschuldigtenproben“ (und -daten), die nur zum Zweck der Unterscheidung von möglichen Täterspuren analysiert worden sind.

Weil diese Situation auch aus der Sicht des LKA unbefriedigend ist, wurde dort eine Interimslösung ins Auge gefasst, wonach Daten, Akten und DNA-Material nach der doppelten Verjährungsfrist gelöscht bzw. vernichtet (= 10/20 Jahre) und Zugriffsrechte auf Einzelpersonen beschränkt werden sollen. Diese Auffanglösung wurde vom Ministerium der Justiz abgelehnt. Sie hätte auch aus der Sicht des LfD das oben dargestellte Grundsatzproblem nicht gelöst, sondern allenfalls abgemildert.

Der LfD hat sich darum bemüht, in einer Stichprobe von Strafverfahrensakten, in denen solche „Altfälle“ dokumentiert waren, herauszufinden, warum die Vernichtungsanordnungen unterblieben sind. Diese Prüfung war langwierig und konnte noch nicht abgeschlossen werden. Die Gesamtproblematik ist Gegenstand von Erörterungen zwischen dem ISM und dem JM. Ein Ergebnis ist dem LfD noch nicht bekanntgegeben worden (s. hierzu auch Tz. 7.1.1.2).

Ein weiteres Problem stellte die Frage dar, wie das LKA in den Fällen verfahren sollte, in denen nach Abschluss der DNA-Analyse zu entscheiden ist, ob die Daten zum Zweck der vorbeugenden Straftatenbekämpfung weiter aufzubewahren sind. Aus der Sicht des LfD muss hier zeitnah entschieden werden, um zu vermeiden, dass Daten Unschuldiger länger als gesetzlich erlaubt gespeichert

werden. Die Verfahrensweise bei diesen sogenannten „Umwidmungen“ von DNA-Analysen aus Verfahren gegen namentlich bekannte Beschuldigte (Js-Verfahren) nach dem Identitätsfeststellungsgesetz in „Nichttrefferfällen“ war derzeit zu zeitaufwändig, um dem gesetzlich vorgegebenen Zeitrahmen der „unverzüglichen“ Vernichtung zu entsprechen. Deshalb hat der LfD gebeten, folgende Verfahrensweise zu erwägen: Das derzeit von den auftragserteilenden Polizeidienststellen verwandte Formular könnte dahingehend erweitert werden, dass bereits bei Übersendung des Probenmaterials von der sachbearbeitenden Polizeidienststelle verfügt werden kann, dass bei „Nichttrefferfällen“ die Analysedaten vernichtet werden können. Wenn so verfahren würde, entfiele das zeitaufwändige (ca. acht Wochen dauernde) Mahnverfahren mit säumigen sachbearbeitenden Polizeidienststellen. Auch hierüber ist bislang noch nicht entschieden worden.

Weiter wurde festgestellt, dass die vorhandenen automatisiert geführten Tagebuchverfahren datenschutzrechtliche Anforderungen nicht oder nur teilweise abgedeckt haben. Dies gilt insbesondere für Protokollierungs-, Wiedervorlage- und Löschfunktionen. Angesichts des vorgesehenen Umstiegs auf eine modernere Lösung, die diese Funktionalitäten bietet, hat der LfD jedoch von einer Problematisierung der auslaufenden jetzigen Lösung abgesehen.

5.9 Einsatzkonzeptionen und neue Datenverarbeitungsverfahren der Polizei zur Vorbereitung der Fußballweltmeisterschaft 2006

Bereits zu Beginn des Jahres 2004 hatte die Polizei mit den Einsatzvorbereitungen für die Fußballweltmeisterschaft 2006, die sich im Bereich Kaiserslautern auf den Zeitraum vom 9. Juni 2006 bis 9. Juli 2006 erstrecken wird, begonnen. Die Polizei informierte den LfD frühzeitig über das erarbeitete Sicherheitskonzept, das neben der Erprobung neuer Datenverarbeitungsverfahren auch den Einsatz von Videokameras umfasst.

Zum Einsatz kommen werden Netzwerkkameras, die über Bildsensoren verfügen und Tag und Nacht einsetzbar sind. Die Geräte nutzen einen Ring-Puffer-Mechanismus, der ältere Aufnahmen nach maximal 48 Stunden mit neuem Material überschreibt. Das gespeicherte Bildmaterial lässt sich über die in die Kamera integrierte Software wiedergeben. Der LfD hat den zu Testzwecken im Mai 2004 begonnenen Probelauf von Aufzeichnungsgeräten geprüft, deren aufgezeichnete Daten (Bildmaterial) in der Pilotphase Prüf- und Ausbildungszwecken dienten. Vom Grundsatz her dürfen nach § 33 Abs. 2 Satz 1 POG personenbezogene Daten nur zu dem Zweck gespeichert und genutzt werden, zu dem sie erhoben wurden. Die Speicherung und Nutzung zu anderen Zwecken ist nur zulässig, soweit sie zu diesem Zweck hätten erhoben werden dürfen. Bei zu Ausbildungszwecken erhobenen Daten stehen nicht gefahrenabwehrende Aspekte im Vordergrund, sondern die Aus- und Weiterbildung der Nutzer hinsichtlich Bedienung und Anwendung der Kamera, Erfassungsbereiche, Bildauflösung, Verwertbarkeit, Geeignetheit des VPN-POL zur Übertragung von Bildsignalen, Bandbreitenbedarf und Übertragungszeitverhalten. Zur Aus- und Fortbildung dürfen gemäß § 33 Abs. 7 Satz 1 POG personenbezogene Daten anonymisiert gespeichert und genutzt werden. Die Anonymisierung kann jedoch unterbleiben, wenn dies dem Aus- und Fortbildungszweck entgegensteht und die jeweiligen Interessen des Betroffenen an der Geheimhaltung seiner personenbezogenen Daten nicht offensichtlich überwiegen. Der Anonymisierung steht entgegen, dass die Testphase gerade darauf ausgerichtet ist, die Darstellungsqualität, Bildauflösung und Verwertbarkeit der Aufzeichnungen zu erproben. Weil die Speicherdauer auf maximal 24 Stunden beschränkt und die Zugriffsberechtigung nur dem engen Kreis der den Einsatz planenden und lenkenden Personen eingeräumt war, konnte von einer Wahrung des Geheimhaltungsinteresses des Betroffenen ausgegangen werden. Insoweit bestanden gegen die getestete Datenerhebung im Rahmen des Fachkonzeptes „Videoüberwachung“ keine datenschutzrechtlichen Bedenken.

Daneben war das Akkreditierungsverfahren, das eine Sicherheitsüberprüfung der Personen vorsieht, die eine Zutrittsbefugnis zu besonders geschützten Bereichen im Rahmen der Fußballweltmeisterschaft erhalten sollen, zu prüfen. Insbesondere war vor dem Hintergrund der Erforderlichkeit, der Verhältnismäßigkeit sowie der Transparenz gegenüber den Betroffenen die Frage von Bedeutung, welche Datenbestände der Polizei, des Verfassungsschutzes oder sonstiger Stellen in welchem Umfang und mit welchen Nutzern jeweils herangezogen werden sollten. Zu dieser Thematik haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer 69. Konferenz am 10. und 11. März 2005 in Kiel eine Entschließung erarbeitet, in der sie für die Eingrenzung der Datenverarbeitung auf das unbedingt erforderliche Maß bei der Fußballweltmeisterschaft 2006 plädieren (vgl. Anlage 14).

5.10 Ein Staatsbesuch in Mainz und der Datenschutz

„Glücklicherweise haben die jüngsten Ereignisse um den Besuch des US-amerikanischen Präsidenten in Mainz klargestellt, dass die Bedenken einiger versprengter Liberaler um den Schutz der Individualrechte vor dem Staat nichts anderes als romantische Verklärungen ewig Gestriger sind, welche die Notwendigkeit moderner Zeiten vollständig verkennen. Darum haben die Mainzer Bürger auch und mit ihnen die bundesrepublikanische Öffentlichkeit klaglos kurzfristige Berufsverbote, Hausarreste und Fahrverbote ertragen.“ (so Professor Dr. Hans-Heiner Kühne, Trier, in seinem Editorial Heft 19/2005 der Neuen Juristischen Wochenschrift)

So und ähnlich äußerten sich auch viele Mainzer Bürger in vielen Leserbriefen. Für den Staatsbesuch des obersten Repräsentanten des mächtigsten Staates der Welt in Mainz wurde seitens der Sicherheitsbehörden eine ganz besondere Bedrohungslage angenommen. Man ging von konkreten Gefahren durch islamistische Zellen und Netzwerke aus, zum andern habe es konkrete Hinweise auf Gewalttäter aus bestimmten Regionen Deutschlands gegeben. Der Verfassungsschutz habe vor militanten Autonomen gewarnt. Die Lage wurde als so ernst eingeschätzt, dass ein richterlicher Beschluss erlassen wurde, der den Einsatz verdeckter Ermittler im Rahmen der zeitgleich durchgeführten Gegendemonstration gestattete.

Scharfschützen waren positioniert. Für am Wahrscheinlichsten wurde ein Giftgasanschlag gehalten. Wenn ein Gegenstand auf das Fahrzeug des Präsidenten geworfen worden wäre, hätte sich der Konvoi des Präsidenten sofort in einen der vorbereiteten Fluchträume zurückgezogen (was eine eigene Gefahr begründet hätte). Besondere Probleme bereitete auch das Verhältnis zu den amerikanischen Sicherheitsbehörden, die eigene Vorstellungen zum erforderlichen Sicherheitsniveau durchsetzen wollten. Vor diesem Hintergrund waren die sicherheitsbehördlichen Aktionen im Vorfeld des Besuchs und am Besuchstag selbst zu sehen.
Angesichts dieser Lage, die eine Gefahr im Sinne des Polizeirechts begründete, waren auch aus Datenschutzsicht keine Einwände gegen allerdings ungewöhnliche Eingriffe in das Datenschutzgrundrecht zu erheben. So wurden die Bewohner ganzer Straßenzüge im Vorhinein überprüft und von der Polizei aufgesucht; ihre Besucher benötigten für den Tag selbst eine besondere Zulassung. Diese zeitlich eng begrenzten datenschutzrechtlichen Eingriffe in die Rechte der Bürger, die im engeren Sicherheitsbereich des Staatsbesuchs wohnten, waren nicht zu verhindern. Die kurzfristig nötigen Datenspeicherungen aus Melderegisterauszügen und Abgleichen mit polizeilichen Informationssystemen wurden jedoch unmittelbar nach Abschluss des Staatsbesuchs, der – wohl auch dank der effizienten polizeilichen Maßnahmen – erfreulicherweise ohne gravierende Zwischenfälle verlief, vernichtet. Die Nutzung dieser Erkenntnisse erfolgte ausschließlich zum Zweck der Sicherung des Staatsbesuchs. Insgesamt kann daher aus datenschutzrechtlicher Sicht eine durchaus positive Bilanz gezogen werden.

Dennoch gab es Einzelfälle, die auch aus der Sicht des LfD nicht in Ordnung waren. So hat die Polizei von sich aus, ohne dass es eines externen Einflusses bedurft hätte, eingeräumt, dass die gewaltsame Öffnung einer Wohnung am Weg des Präsidenten in Abwesenheit der Wohnungsbesitzerin rechtswidrig war. Dieser „Einbruch“ war geschehen, um ein Transparent mit der Aufschrift „Not welcome, Mr. Bush“ zu entfernen. Der Polizeipräsident entschuldigte sich öffentlich bei der Betroffenen.

In einem weiteren Fall hat ein Polizeibeamter im Rahmen eines Besuchs bei den Bewohnern von an der Besuchsroute liegenden Häusern eine unangemessene Bemerkung gemacht. Er besuchte ein Büro mit einigen Mitarbeitern. Dabei fiel ihm ein Name auf einem an einem Zimmer befindlichen Namensschild auf und er fragte: „Ach, ist der Dr. xy hier?“ Auf die Auskunft hin, dieser sei nicht anwesend, und auf die Gegenfrage, warum er das wissen wolle, erklärte er, der Leserbrief des Dr. xy in der örtlichen Zeitung sei ja starker Stoff gewesen. Der Betroffene fühlte sich dadurch bei seinen Kollegen diffamiert; diese hätten den Eindruck gewonnen, sein Leserbrief sei „polizeiwidrig“, jedenfalls sei er wohl geeignet gewesen, ihn ins Blickfeld der Polizei zu rücken. Es ergab sich, dass es sich hier um eine rein private Bemerkung des betroffenen Beamten gehandelt hatte. Das Innenministerium entschuldigte sich beim Betroffenen. Der LfD stellte fest, dass auch keine Daten des Betroffenen durch die Polizei gespeichert wurden oder werden.

In zwei weiteren Fällen steht eine Klärung noch aus.

5.11 Eingaben

5.11.1 Recht des Betroffenen auf Auskunft

Weil ihm auf wiederholte Auskunftsersuchen an eine Polizeiinspektion keine Auskunft zu über seine Person gespeicherte Daten erteilt wurde, ersuchte ein Betroffener den LfD um Hilfe bei der Durchsetzung seines Auskunftsanspruchs. Das Recht des Bürgers auf Auskunft gegenüber der Polizei ist im Einzelnen in § 40 POG (ehemals § 25 f POG) geregelt. In dem in Rede stehenden Ersuchen waren die Daten im automatisierten Verfahren der Polizei gelöscht worden, nachdem der Betroffene seinen Auskunftsantrag gestellt hatte, da die rechtliche Bewertung durch die Polizei selbst die Unzulässigkeit der Informationsspeicherung ergeben hatte. Nach Intervention des LfD teilte die Polizeibehörde dem Betroffenen mit, welche Daten im automatisierten Verfahren gelöscht worden waren. Dazu nutzte sie den zu diesem Zeitpunkt noch vorhandenen Aktenrückhalt, der anlässlich des Auskunftsantrags entstanden war. Inzwischen ist nach Fristablauf auch dieser Aktenrückhalt vernichtet worden.

5.11.2 Unterrichtung der falschen Institution über die Durchsuchung von Arbeitsräumen; Angemessenheitsfragen bei einer erkennungsdienstlichen Behandlung

Eine Petentin war der Auffassung, durch die Vorgehensweise der Polizei im Zusammenhang mit der Durchsuchung von Arbeitsräumen und bei einer erkennungsdienstlichen Behandlung seien ihre Datenschutzrechte verletzt worden. Wie die Recherchen des LfD ergaben, war von der Polizei tatsächlich vor der Durchsuchung des Arbeitsplatzes (versehentlich) anstelle des wahren Arbeitgebers die falsche Institution über die Maßnahme unterrichtet worden, weil der ermittelnde Polizeibeamte eine irreführende Angabe über den Arbeitgeber zur (nicht ausreichend überprüften) Grundlage von Durchsuchungsmaßnahmen und damit zusammenhängenden Datenübermittlungen gemacht hatte. Die Auswirkungen waren zwar im Ergebnis durchaus gewichtig, weil rufschädigende Informationen über die Petentin an unzuständige Stellen gelangten. Das Versäumnis selbst allerdings beruhte auf der Sorgfaltspflichtverletzung eines Einzelnen. Zudem räumte die Polizei den Fehler ein, so dass damit zu rechnen ist, dass künftig sorgfältiger gearbeitet werden wird. Deshalb war von einer förmlichen Beanstandung gem. § 25 Abs. 2 LDSG hinsichtlich der Datenübermittlung an den falschen Arbeitgeber abzusehen.

Anders war die Durchführung der erkennungsdienstlichen Maßnahme zu beurteilen. Wegen der unzureichenden und teilweise widersprüchlichen polizeilichen Dokumentationen und Darstellungen des Sachverhalts bestand zwar keine Möglichkeit, den Hergang der erkennungsdienstlichen Behandlung exakt zu rekonstruieren. Der Petentin wurde jedenfalls eine Speichelprobe entnommen. Es ist außerdem davon auszugehen, dass in einem separaten Raum eine Inaugenscheinnahme der Körperoberfläche der Petentin

durch eine Bedienstete ohne Anwesenheit Dritter stattgefunden hat. Zwar dürfen nach § 81 b 1. Alt. StPO, „soweit es für die Zwecke der Durchführung des Strafverfahrens (…) notwendig ist, Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden". Eine Entkleidung zur Feststellung unveränderlicher körperlicher Merkmale lag im vorliegenden Fall (einem Ermittlungsverfahren wegen Beleidigung und Sachbeschädigung) – unabhängig davon, ob eine völlige oder nur eine partielle Entkleidung verlangt wurde – außerhalb des Angemessenen und Vertretbaren.

Außerdem enthielt die der Petentin übersandte Vorladung zur erkennungsdienstlichen Behandlung keinen ausdrücklichen Hinweis auf den vorliegenden richterlichen Beschluss zur Speichelprobenentnahme gem. §§ 81a ff StPO, eine Rechtsbehelfsbelehrung bezüglich der beabsichtigten ED-Behandlung (gem. § 81 b 1. Alt. StPO) fehlte.

Dieses Vorgehen beanstandete der LfD als Verstoß gegen datenschutzrechtliche Vorschriften.

5.12 Veröffentlichung von Beamten-Lichtbildern im Internet

Im aktuellen Berichtszeitraum stellte sich die Frage, ob und in welchem Umfang Bezirksbeamtendaten im Internet veröffentlicht werden dürfen. Aus der Sicht des LfD wird der Bezirksbeamte als Repräsentant des Staates tätig und hat im Rahmen der Kontaktpflege eine Veröffentlichung seines Fotos in dem räumlich begrenzten Umfeld, in dem er tätig wird, hinzunehmen. Eine Veröffentlichung im Internet erscheint allerdings nicht unabdingbar erforderlich oder geboten und ist nach Auffassung des LfD gegen den Willen des Beamten nicht zulässig. Das Ministerium des Innern und für Sport teilt die Auffassung des LfD.

5.13 Rasterfahndung

Zum 19. Tätigkeitsbericht (Tz. 5.2) ist nachzutragen, dass Inhalt und Verbleib von Dokumentationsdaten der Rasterfahndung sowie die personenbezogenen Informationen, die aufgrund von Ergebnissen der Rasterfahndung zu Zwecken der Gefahrenabwehr oder Strafverfolgung gespeichert wurden, aber auch die im Rahmen der Benachrichtigung Betroffener archivierten Daten Gegenstand örtlicher Feststellungen bei einem Polizeipräsidium und dem Landeskriminalamt (als Koordinationsstelle) waren. Im Ergebnis wurde festgestellt, dass nach ersten polizeilichen Bewertungen und „Schläfer-Ausschlüssen" bis zum November 2004 sukzessive die Löschung aller Daten, Datenbanken und Dokumente der Rasterfahndung vorgenommen und die Dokumentation der Löschung anonymisiert dem behördlichen Datenschutzbeauftragten übergeben worden waren. Ausgenommen waren nur einige wenige weiterhin relevante Datensätze. Personen, gegen die nach automatisiertem Dateiabgleich und büromäßiger Abklärung weitere Maßnahmen zur Gefahrenabwehr getroffen worden waren, wurden von der Polizei über die getroffenen Maßnahmen informiert. Insgesamt stufte die Polizei die Resonanz der Betroffenen als äußerst gering ein, Widerspruchsverfahren waren nicht eingeleitet worden. Die nachvollziehbare Dokumentation der Datenreduzierung und -löschung der unter dem Aspekt des Datenschutzes besonders bedeutsamen Verarbeitungsschritte der im Rahmen der Rasterfahndung gewonnenen Daten ermöglichte eine umfassende datenschutzrechtliche Kontrolle. Defizite waren nicht festzustellen.

6. Verfassungsschutz

6.1 Auskunftsanspruch gegenüber dem Verfassungsschutz

Auch im aktuellen Berichtszeitraum wandten sich wiederum Betroffene an den LfD, um die Zulässigkeit von Auskunftsverweigerungen des Verfassungsschutzes überprüfen zu lassen. Dieser berief sich in diesen Fällen darauf, dem Ersuchen könne ohne Aufgabengefährdung der Verfassungsschutzbehörden nicht entsprochen werden. Im Einvernehmen mit dem Verfassungsschutz konnte durch das Erteilen einer Teilauskunft, die sich auf die Tatsache von Speicherungen generell bezog, sowohl dem Rechtsanspruch auf Auskunft als auch den berechtigten Interessen des Verfassungsschutzes (die insbesondere auch den Quellenschutz zum Gegenstand haben) Rechnung getragen werden.

Im Zusammenhang mit diesen Eingaben hat der LfD auch regelmäßig geprüft, ob die Informationsspeicherungen des Verfassungsschutzes den rechtlichen Vorgaben entsprochen haben. Es ergab sich kein Anlass für Beanstandungen.

6.2 Islamistendatei

Unter den Innenministern von Bund und Ländern ist es unumstritten, dass zur Verbesserung der vorbeugenden Terrorismusbekämpfung eine bessere Unterrichtung der Sicherheitsbehörden untereinander über die jeweils dort vorhandenen Erkenntnisse über als gefährlich einzustufende Personen erfolgen soll. Über den Weg dorthin besteht insofern Einigkeit, als eine gemeinsame Datei aller beteiligten Sicherheitsbehörden (insbesondere die Polizeien und die Ämter für Verfassungsschutz des Bundes und der Länder) für sinnvoll gehalten wird.

Streit besteht allerdings darüber, welchen Inhalt diese Datei haben soll: soll es eine sogenannte „Indexdatei" mit Hinweisen auf jeweils aktenbesitzende Stellen sein, oder sollen inhaltliche Erkenntnisse über Einzelpersonen gespeichert und abgerufen werden können?

Aus der Sicht des Datenschutzes sind in diesem Zusammenhang folgende Punkte zu betonen:

Eine unterschiedslose Zusammenlegung sämtlicher Informationsbestände aller Sicherheitsbehörden darf es nicht geben. Vielmehr muss die Datenübermittlung, auch wenn sie auf neuer technischer Basis erfolgen soll, den Anforderungen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung Rechnung tragen: So dürfen nur die Informationen weitergegeben werden, die zur Bekämpfung des islamistischen Terrorismus erforderlich sind. Die Daten müssen einer strikten Zweckbindung unterworfen sein, wobei Informationen, die auf Basis besonderer Eingriffsermächtigungen erhoben wurden – etwa bei der Telefonüberwachung – besonders zu kennzeichnen sind. Auch muss erkennbar sein, welche Stelle die Daten weitergegeben hat. Der Abruf von Daten ist lückenlos zu protokollieren und muss einer effektiven datenschutzrechtlichen Kontrolle zugänglich sein. Die Einführung gemeinsamer Dateien darf nicht zu einer Schwächung rechtsstaatlicher Positionen führen.

Einem weitergehenden Informationsaustausch zwischen den Sicherheitsbehörden stehen häufig Quellenschutzerfordernisse der Nachrichtendienste oder föderale Zuständigkeiten entgegen. Hieran würden auch gemeinsame Dateien, wie die vorgeschlagene Islamistendatei, wenig ändern. Die verschiedenen Sicherheitsbehörden haben unterschiedliche, gesetzlich normierte Aufgaben und Befugnisse. Es besteht ein erheblicher Unterschied zwischen der Beobachtung und Analyse verfassungsfeindlicher Bestrebungen durch den Verfassungsschutz einerseits und der strafrechtlichen Aufklärung und Gefahrenabwehr der Strafverfolgungsbehörden und der Polizei andererseits. Die Nachrichtendienste arbeiten mit nachrichtendienstlichen Mitteln zur Gewinnung teils sehr sensibler Daten, wie etwa Quellenmaterial oder Auslandsinformationen, die nur sehr eingeschränkt zur repressiven Kriminalitätsbekämpfung geeignet sind. Sie sind zudem weitgehend der gerichtlichen Kontrolle entzogen.

Die technische Optimierung der gesetzlich zugelassenen Informationsbeziehungen ist selbstverständlich auch aus datenschutzrechtlicher Sicht zulässig, um auf diese Weise Informationsdefizite zu vermeiden.

6.3 Anmeldungen des Verfassungsschutzes zum Verfahrensregister beim LfD; technisch-organisatorische Datenschutzmaßnahmen innerhalb des Verfassungsschutzes

Anlässlich örtlicher Feststellungen beim Verfassungsschutz des Landes wurde das beim LfD geführte Verzeichnis der automatisierten Verfahren des Landesverfassungsschutzes aktualisiert.

Außerdem wurden Anregungen zur internen Abschottung von Dokumenten formuliert, die auf dem DV-System der Verfassungsschutzabteilung gespeichert werden. Diesen Anregungen ist der Verfassungsschutz nachgekommen. Er beabsichtigt, ein neues Verfahren zur Dokumentenverwaltung einzuführen, das auch ein neues an Benutzergruppen orientiertes Rechtekonzept vorsieht. Dem LfD wurde zugesichert, ihn zeitnah zu unterrichten und ihm Gelegenheit zur Stellungnahme zu geben.

6.4 Mitwirkung an Zuverlässigkeitsüberprüfungen

In Folge erhöhter Sicherheitsanstrengungen zur Vorsorge gegenüber terroristischen Gefahren wurden Sicherheitsüberprüfungen aller Bediensteter, die in besonders gefährdeten Anlagen tätig sind, verstärkt durchgeführt. Eine größere Zahl von Eingaben betraf die Frage, ob denn die Arbeitnehmer verpflichtet seien, zum Zweck solcher Überprüfungen höchstpersönliche Angaben zu machen, die über ihren Arbeitgeber an den deutschen Verfassungsschutz oder – im Falle einer Tätigkeit der einsetzenden Firma in Liegenschaften der US-Streitkräfte – an Sicherheitsbehörden der ausländischen Macht gelangen würden.

Der LfD hat in diesen Fällen wie folgt Stellung genommen: Die amerikanischen Dienststellen unterliegen der Kontrollkompetenz des LfD ebenso wenig wie der (u. U. bei solchen Sicherheitsüberprüfungen mitwirkende) deutsche privatrechtlich organisierte Arbeitgeber von Betroffenen. Seine Zuständigkeit beschränkt sich auf die öffentlichen Stellen (die Behörden) des Landes. So hat sich der LfD mit der Situation von Beschäftigten des Landesbetriebs Liegenschafts- und Baubetreuung (LBB) befasst, die in US-amerikanischen Einrichtungen im Auftrag ihres Arbeitgebers tätig sind und denen Fingerabdrücke zur Fertigung von Sicherheitsausweisen abverlangt worden sind.

Das Verfahren der Sicherheitsüberprüfungen, soweit diese durch deutsche Stellen durchgeführt werden, ist gesetzlich in den Sicherheitsüberprüfungsgesetzen des Bundes (dieses gilt für die Bundesbehörden) und des Landes (das für die Landesbehörden gilt) geregelt. Regelmäßig wirkt der Landesverfassungsschutz unter Nutzung der bei ihm vorhandenen Erkenntnisse an solchen Sicherheitsüberprüfungen mit. In allen Fällen werden nahezu identische Formulare eingesetzt. Ob Befragungen im persönlichen Lebensumfeld der zu prüfenden Person erfolgen und ob deren Lebenspartner einbezogen wird, hängt dabei vom Einzelfall ab; grundsätzlich ist auch dies vorgesehen, da die Situation des Lebenspartners durchaus den Betroffenen selbst beeinflussen und ihn zum Sicherheitsrisiko machen kann. Deshalb werden auch entsprechende Fragen (deren Beantwortung allerdings die Zustimmung des Lebenspartners voraussetzt) gestellt.

An den Arbeitgeber werden Erkenntnisse der mitwirkenden Sicherheitsbehörden nur weitergegeben, wenn sie Sicherheitsbedenken begründen. Letztlich sind diese Datenübermittlungen auch gerichtlich überprüfbar.

Der LBB setzt Mitarbeiter im Bereich der Liegenschaften der US-Stationierungsstreitkräfte ein. Die Mitarbeiter des LBB stehen nur zum LBB in unmittelbaren rechtlichen (arbeitsvertraglichen oder beamtenrechtlichen) Beziehungen. Voraussetzung dieses externen Einsatzes ist allerdings, dass die US-Behörden eine Sicherheitsüberprüfung der einzusetzenden Beschäftigten durchführen, die unter Mitwirkung des LBB erfolgt.

Der LfD kann in diesem Zusammenhang beurteilen, ob der LBB befugtermaßen an der Sicherheitsüberprüfung seiner in amerikanischen Liegenschaften eingesetzten Beschäftigten durch die US-Dienststellen durch die Übermittlung von ausgefüllten Sicherheitserklärungen mitwirkt. Dies ist aus der Sicht des LfD gem. § 17 Abs. 3 Nr. 2 LDSG der Fall, wenn die Übermittlung für die Durchführung des Beschäftigungsverhältnisses zwischen den Betroffenen und dem LBB erforderlich ist.

Zur Erfüllung seiner Aufgaben ist der LBB darauf angewiesen, dass seine Mitarbeiter Zutritt zu amerikanischen Liegenschaften erhalten. Die dafür erforderlichen Datenerhebungen der US-Behörden sind nicht offensichtlich rechtswidrig; es gibt auch für die Beschäftigung von Personen in einem sicherheitsrelevanten Umfeld, das zum deutschen Hoheitsbereich gehört, vergleichbare Überprüfungen. Die vorliegenden Datenerhebungen dürften im Wesentlichen den nach den genannten Gesetzen erfolgenden Datenerhebungen der deutschen Sicherheitsbehörden entsprechen. Auch die Erhebung und Nutzung von Fingerabdrücken für Ausweise, die den Zugang zu sicherheitsrelevanten Bereichen ermöglichen sollen, ist nicht unverhältnismäßig oder rechtswidrig.

Selbstverständlich aber muss jeder Einzelne entscheiden, ob er die mit einem solchen Verfahren einhergehenden Belastungen im Interesse seines Arbeitsplatzes akzeptiert.

7. Justizbereich

7.1 Strafrecht/Strafverfahrensrecht

7.1.1 DNA-Untersuchungen im Strafverfahren

7.1.1.1 Gesetzliche Neuregelungen

Die Diskussion um die gesetzliche Ausgestaltung der DNA-Analyse im Strafverfahren hat sich im Berichtszeitraum fortgesetzt. Sie ist mit Gesetz vom 12. August 2005 (BGBl. I, 2360), das am 1. November 2005 in Kraft tritt, zu einem vorläufigen Abschluss gekommen.

Künftig entfällt der Richtervorbehalt für anonyme Spuren. Gleiches gilt, wenn der Betroffene einwilligt. Weiterhin sieht das Gesetz vor, eine DNA-Analyse für Zwecke künftiger Strafverfolgung nicht nur bei erheblichen Straftaten und allen Sexualdelikten, sondern auch bei wiederholter Begehung nicht erheblicher Straftaten zuzulassen, weil viele Täter, die schwere Straftaten begehen, zuvor mehrfach mit einfacheren Taten auffällig geworden seien. Eine völlige Gleichstellung des genetischen Fingerabdrucks mit dem herkömmlichen und damit den generellen Verzicht auf qualifizierte Anforderungen an Anlasstat und Negativprognose und eine gänzliche Streichung des Richtervorbehalts wurde aus Verfassungsgründen nicht geschaffen. Zugleich wurde der erweiterte Anwendungsbereich mit Regelungen flankiert, die die Rechtsstaatlichkeit des Verfahrens weiter absichern sollen. So wird der Reihengentest auf eine gesetzliche Grundlage gestellt. In den sogenannten Umwidmungsfällen sieht das Gesetz vor, Betroffene künftig über die Speicherung in der DNA-Analyse-Datei zu informieren und auf die Möglichkeit hinzuweisen, die Speicherung gerichtlich überprüfen lassen zu können.

Der LfD hat gegen dieses Gesetzgebungsvorhaben keine Bedenken erhoben. Aus seiner Sicht ist damit eine praxisgerechte datenschutzkonforme Weiterentwicklung dieses wichtigen, unter dem Gesichtspunkt des Persönlichkeitsschutzes allerdings gefährlichen Ermittlungsinstruments geschaffen worden.

7.1.1.2 Datenschutzfragen beim praktischen Vollzug

Die Überprüfung einer Stichprobe von Strafverfahrensakten, in denen DNA-Analysemaßnahmen zur Strafverfolgung angeordnet worden waren (s. auch Tz. 5.8), ergab folgende datenschutzrechtlich relevante Fragestellungen:

Wie lange ist die Aufbewahrung von Körperproben namentlich bekannter Urheber „erforderlich“ im Sinn der gesetzlichen Regelung (§ 81 a Abs. 3 StPO)? Welche Gesichtspunkte könnten nach Durchführung der molekulargenetischen Analyse und Erstellung der Identifizierungsmuster die weitere Aufbewahrung von Körperproben namentlich bekannter Urheber rechtfertigen? Ist in solchen Fällen die theoretische Möglichkeit, dass eine Wiederholungsanalyse zum Ausschluss von Fehlern verlangt werden könnte, ausreichend?

Was heißt „unverzüglich“? Wann ist von der Staatsanwaltschaft über die Vernichtung der DNA-Untersuchungsproben (der Körpermaterialien namentlich bekannter Beteiligter: Beschuldigte, Zeugen, Opfer, Dritte) zu entscheiden? M. a. W.: wann ist „unverzüglich“, sobald die Proben für Zwecke eines anhängigen Strafverfahrens nicht mehr erforderlich sind i. S. v. § 81 a Abs. 3 zweiter Halbsatz StPO? Ist dies erst mit Beendigung des Erkenntnisverfahrens der Fall oder gibt es Fälle, z. B. bei molekulargenetischem Ausschluss eines Verdächtigen als Spurenverursacher, in dem diese Vernichtung schon vorher, im laufenden Verfahren erfolgen müsste?

Welche verfahrenstechnischen organisatorischen Mechanismen garantieren, dass eine den gesetzlichen Vorgaben entsprechende Entscheidung der jeweiligen Staatsanwaltschaft (oder/und der zuständigen Polizeibehörde) über die Vernichtung von Körperproben im Rahmen einer DNA-Analyse unverzüglich erfolgt, die gem. § 81 e StPO (im Rahmen eines laufenden Strafverfahrens) durchgeführt wurde?

Welche verfahrenstechnischen organisatorischen Mechanismen garantieren, dass eine den gesetzlichen Vorgaben entsprechende Entscheidung der jeweils zuständigen Polizeibehörde über eine etwa notwendige Umwidmung von DNA-Identifizierungsmustern aus einem konkreten Strafverfahren für polizeiliche vorbeugende Zwecke (künftig mit Unterrichtungspflicht gegenüber dem Betroffenen gem. § 81 g Abs. 3 StPO) getroffen wird?

Wie lange sind die DNA-Verformelungen (DNA-Identifizierungsmuster) beim LKA aufzubewahren? Unter welchen Voraussetzungen werden – zunächst – nicht auswertbare Spuren (z. B. Haare ohne Wurzeln) erneut – in nicht aufgeklärten Fällen – mithilfe zwischenzeitlich verbesserter Methoden analysiert? Muss die Initiative von der ermittelnden Polizeidienststelle ausgehen? Kann das LKA als Untersuchungsstelle hier Anregungen geben? Müsste ein erneuter richterlicher Beschluss ergehen?

Der LfD bemüht sich um die Klärung dieser Fragen.

7.1.2 Die akustische Wohnraumüberwachung:

7.1.2.1 Rechtliche Entwicklung

Nach der StPO dürfen Abhörmaßnahmen in Wohnungen unter engen Voraussetzungen durchgeführt werden. Mit seinem Urteil vom 3. März 2004 (Az.: 1 BvR 2378/98) hat das Bundesverfassungsgericht klargestellt, dass dabei nicht in den innersten Bereich der privaten Lebensgestaltung Verdächtiger eingegriffen werden darf (zu vergleichbaren Fragen im Polizeirecht s. Tz. 5.1).

Der Bundesgesetzgeber hat diese Vorgaben nunmehr auch in den Gesetzestext übernommen (Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 – akustische Wohnraumüberwachung – vom 24. Juni 2005, BGBl. I, 1841). Wesentliche Inhalte der neuen Regelung sind:

Es muss der Verdacht einer besonders schweren Straftat gegeben sein. Dies ist nur bei solchen Straftaten der Fall, für die das Gesetz eine Freiheitsstrafe von mehr als fünf Jahren vorsieht. Insbesondere sind hier Kapitaldelikte wie Mord und Totschlag, banden- oder gewerbsmäßige Verbreitung von Kinderpornografie sowie Straftaten terroristischer Vereinigungen einbezogen.

Vertrauliche Gespräche zwischen sich nahestehenden Personen, die keinen Bezug zu Straftaten aufweisen („Kernbereich privater Lebensgestaltung"), dürfen nicht abgehört werden. Die akustische Wohnraumüberwachung darf deshalb nur noch angeordnet werden, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass keine Äußerungen aus diesem absolut geschützten Bereich erfasst werden. Beim Abhören von Gesprächen in Privatwohnungen muss deshalb in der Regel live mitgehört werden, um das Abhören unverzüglich zu unterbrechen, wenn solche Gespräche geführt werden.

Das Abhören von Gesprächen mit Berufsgeheimnisträgern (Rechtsanwälten, Notaren, Wirtschaftsprüfern, Steuerberatern, Ärzten, Mitarbeitern von Beratungsstellen für Schwangerschaftskonflikte oder Betäubungsmittelabhängigkeit, Abgeordneten, Medienmitarbeitern etc.) ist unzulässig. Werden im Einzelfall solche Gespräche dennoch versehentlich erfasst, so sind die Aufzeichnungen zu löschen. Die erlangten Informationen dürfen grundsätzlich nicht verwertet werden, ausgenommen zur Abwehr bestimmter schwerwiegender Gefahren, z. B. durch bevorstehende terroristische Anschläge.

Die akustische Wohnraumüberwachung darf nur von eigens dafür eingerichteten spezialisierten Kammern bestimmter Landgerichte angeordnet werden. Die anordnende Kammer ist über den Verlauf der Maßnahme zu unterrichten. Damit ist sichergestellt, dass die Kammer jederzeit die Unterbrechung der Maßnahme oder deren Abbruch anordnen kann.

Nach dem Abschluss der Überwachung sind die betroffenen Personen (Beschuldigte, sonstige überwachte Personen, Inhaber und/oder Bewohner der überwachten Wohnung) zu benachrichtigen, damit sie die Möglichkeit erhalten, die Rechtmäßigkeit der Anordnung und Durchführung der Maßnahme nochmals gerichtlich überprüfen zu lassen.

Die Landesjustizverwaltungen müssen über die Bundesregierung dem Deutschen Bundestag jährlich detailliert über die Maßnahmen der akustischen Wohnraumüberwachung berichten. Diese Berichtspflicht wird auf 12 Berichtspunkte ausgebaut, um die parlamentarische Kontrolle der akustischen Wohnraumüberwachung nach Art. 13 Abs. 6 GG zu stärken.

Der LfD hält diese Regelungen insgesamt für verfassungskonform. Die Schwierigkeiten der praktischen Umsetzung dürften allerdings erheblich sein.

7.1.2.2 Evaluierung

Schon lange vor der zitierten Verfassungsgerichtsentscheidung hatte das Bundesjustizministerium – auch einer Anregung der Datenschutzbeauftragten folgend – eine Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Auftrag gegeben, um in Erfahrung zu bringen, wie effektiv einerseits solche Maßnahmen zur Straftatenaufklärung sind und andererseits, welche „Kosten" in Bezug auf Grundrechtseingriffe damit verbunden sind. Diese Untersuchung wurde im Berichtszeitraum vorgelegt.

Unter Federführung des LfD hat sich eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder mit der Frage befasst, ob dieses Gutachten die aus datenschutzrechtlicher Sicht bedeutsamen Fragen beantworten konnte. Die Arbeitsgruppe ist zu folgendem Ergebnis gekommen:

Mit dem Gutachten hat das Bundesjustizministerium den Versuch unternommen, die Wirksamkeit einer aus der Sicht des Grundrechtsschutzes äußerst bedeutsamen, weil intensiv den Kernbereich der geschützten Privatsphäre berührenden Ermittlungsmaßnahme zu evaluieren. Dies ist aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen.

Allerdings ist festzustellen, dass es sogar mit den Mitteln einer zeit- und arbeitsaufwändig erstellten Analyse unter Beiziehung der Akten und unter Beteiligung der die Maßnahme praktisch durchführenden Ermittlungspersonen (im Wege von Experteninterviews) nicht gelungen ist (möglicherweise auch nicht gelingen konnte), auf alle aus der Sicht des Datenschutzes relevanten Fragen Antworten zu finden. Dies ist zum größten Teil sicherlich auf die in den Akten nur unzureichend vorhandene Dokumentation der Maßnahmen zurückzuführen.

Beispielsweise konnten im Gutachten folgende Aspekte nur wenig aufgehellt werden:

- Die Zahl der von Abhörmaßnahmen tatsächlich Betroffenen (deren mündliche Äußerungen also aufgezeichnet und von Polizeibeamten zur Kenntnis genommen worden sind) konnte nicht eindeutig festgestellt werden;
- Die Stellung der Betroffenen zueinander war oftmals nicht feststellbar; damit konnte auch die Frage nicht geklärt werden, in welche Vertrauensverhältnisse jeweils konkret eingegriffen wurde und wie dies jeweils zu gewichten war. Die Frage, ob die Gesprächspartner z. B. Verwandte, Freunde, Bekannte oder Geschäftspartner waren, ist aber für die Beurteilung, wie intensiv der in der Abhörmaßnahme liegende Grundrechtseingriff war, wesentlich;
- Das Gutachten konnte auch keine detaillierten und systematisierten Angaben zu den abgehörten Gesprächsinhalten machen, z. B. dazu, in welchem Umfang Gespräche abgehört wurden, die den Intimbereich der abgehörten Personen betrafen;
- Es konnten keine genauen Angaben über die Zahl der abgehörten Gespräche/Kommunikationsvorgänge oder die tatsächliche genaue Abhördauer oder auch nur die Dauer der Anwesenheit der Zielpersonen in den abgehörten Räumen gemacht werden;
- Ebenso fehlen genauere Angaben über die jeweils überwachten Räumlichkeiten: handelte es sich um alle Räume einer Wohnung oder nur um bestimmte Räume, ggf. welche?

Auch die Frage, wie erfolgreich die Maßnahmen jeweils waren, ist auf der Grundlage des Gutachtens nicht eindeutig zu beurteilen. Das Gutachten spricht von 30 % erfolgreichen Maßnahmen. Darunter sind allerdings auch die nur „bedingt“ und die „mittelbar“ erfolgreichen, die das Ausgangsverfahren nicht unmittelbar förderten.

Es ist deshalb festzustellen, dass trotz dieses verdienstvollen Evaluationsversuchs Fragen aus der Sicht des Datenschutzes offenbleiben, die für die Bewertung dieses intensiven strafverfahrensrechtlichen Eingriffs bedeutsam sind.

Das Gutachten hat aber ungeachtet dessen wichtige Erkenntnisse geliefert, die aus datenschutzrechtlicher Sicht sowohl bei der praktischen Umsetzung als auch bei der künftigen gesetzgeberischen Ausgestaltung dieser Maßnahme beachtet werden müssen:

- Nach dem Gutachten sind in einem erheblichen Teil der Fälle die Betroffenen in den Verfahrensakten nicht dokumentiert worden; diese konnten also nicht benachrichtigt werden. Auch bei einem erheblichen Prozentsatz der bekannten Betroffenen war nicht feststellbar, dass sie entsprechend der gesetzlichen Regelungen über die durchgeführte Maßnahme unterrichtet wurden. Es ist also darauf hinzuwirken, dass die gesetzlichen Vorgaben zur Benachrichtigung umgesetzt werden.
- Unklarheiten bestehen darüber, wer als Betroffener bzw. Beteiligter der Abhörmaßnahme anzusehen ist. Der Gesetzgeber sollte klarer regeln, dass auch alle betroffenen Dritten (auch die „unvermeidbar betroffenen“) zu benachrichtigen sind.
- Den Anträgen auf Zurückstellung der Benachrichtigung wurde nicht selten trotz einer nur unzureichenden Begründung vom entscheidungsbefugten Gericht stattgegeben. Auf eine ausreichende Begründung sowohl des Antrags wie der gerichtlichen Entscheidung ist zu achten.
- Es erfolgte häufig keine ausreichende Dokumentation der Maßnahme. Aus Gründen der Ermöglichung von Evaluationen, der effektiven Erfüllung der Benachrichtigungspflicht und der damit verbundenen Ermöglichung eines effektiven Rechtsschutzes sowie der Nachvollziehbarkeit von Löschungs- und Vernichtungspflichten hat eine solche Dokumentation aber aus der Sicht des Datenschutzes zu erfolgen; sie sollte gesetzlich umfassender vorgeschrieben werden.
- Die Auswertungsprotokolle wurden nicht immer gesondert gekennzeichnet. Eine solche Kennzeichnung wird aber vom BVerfG als wesentliche verfahrenssichernde Maßnahme für den Grundrechtsschutz gefordert und ist nunmehr auch gesetzlich vorgesehen. Dies ist in der Praxis zu beachten.
- Die Vernichtung der Aufzeichnungsmedien ist – entgegen der bestehenden gesetzlichen Regelung – nicht immer ausreichend protokolliert worden. Auch hier besteht Verbesserungsbedarf.

In Bezug auf den Straftatenkatalog, der Anlass einer solchen Maßnahme sein kann, hat das BVerfG bereits eine deutliche Reduktion unter Zugrundelegung des Maßstabs einer erheblichen Strafandrohung gefordert. Das Gutachten weist darauf hin, dass ein ganz erheblicher Teil der gesetzlich genannten Straftatbestände in keinem einzigen Fall im Untersuchungszeitraum zur Grundlage einer Abhörmaßnahme gemacht worden ist. Vor diesem Hintergrund fordern die Datenschutzbeauftragten, den Straftatenkatalog auch unter dem Aspekt seiner Erforderlichkeit kritisch zu prüfen.

Unabhängig davon sollte der Straftatbestand des besonders schweren Falls der Bestechlichkeit und Bestechung aus dem Katalog der möglichen Anlassstraftaten herausgenommen werden, da dieser nicht im Katalog der eine Telekommunikationsüberwachung begründenden Straftaten enthalten ist. Damit besteht ein nicht akzeptabler Wertungswiderspruch; zudem wird die Gefahr von Umgehungsmaßnahmen begründet.

Fälle der Zweckänderung von erhobenen Daten für Maßnahmen der Gefahrenabwehr sind im Gutachten nicht berichtet worden. Aus der Sicht des Datenschutzes besteht deshalb auch kein Anlass, ausdrücklich zu regeln, dass eine solche Zweckänderung sogar für solche Daten zulässig sein soll, die einem absoluten Verwertungsverbot unterliegen. Jedenfalls sind entsprechende Ausnahmen auf extreme Gefahrensituationen zu begrenzen.

7.1.3 Eingaben im Zusammenhang mit Strafverfahren

Zunächst ist hervorzuheben, dass die Staatsanwaltschaften des Landes den Informationsbedürfnissen des LfD in allen Fällen, in denen er Anfragen hatte und Akteneinsicht erbat, zügig nachgekommen sind. Probleme, die in diesem Zusammenhang in der Vergangenheit gelegentlich aufgetreten waren, waren im Berichtszeitraum nicht mehr festzustellen.

7.1.3.1 Durchsuchung in einem Fall des Verdachts der Beleidigung?

Mitunter erhält der LfD Eingaben, die sich auf richterlich angeordnete Ermittlungsmaßnahmen der Strafverfolgungsbehörden beziehen. Während laufender Strafverfahren sieht der LfD ohnehin grundsätzlich von einer Intervention ab, wenn es sich nicht um spezifische Datenschutzfragen bei der Nutzung der automatisierten Datenverarbeitung handelt oder sonst außergewöhnliche Umstände vorliegen. Aber auch nach Abschluss von Strafverfahren sind diejenigen Handlungen seiner Kontrollkompetenz entzogen, die als richterliche Tätigkeiten anzusehen sind. Dazu gehört z. B. die Frage, ob eine Durchsuchung zu Recht angeordnet worden ist. Nicht dem richterlichen Verantwortungsbereich zuzurechnen sind allerdings – solange der Betroffene diese Fragen nicht gesondert richterlich überprüfen lässt – die Art und Weise sowie der konkrete Zeitpunkt einer Durchsuchung und die Frage, ob bestimmte beschlagnahmte Gegenstände zu Recht beschlagnahmt wurden.

In einem konkreten Fall hatte der LfD Veranlassung, diese Gesichtspunkte nach Abschluss des strafgerichtlichen Verfahrens zu überprüfen. Hintergrund war, dass ein Junggeselle mittleren Alters durch die wöchentlich mit Foto erscheinende Kolumne einer hübschen Journalistin dazu veranlasst wurde, ihr brieflich anonym seine Sympathie auszudrücken. Dies geschah zwar deutlich, aber ohne beleidigende Formulierungen (wie es später auch das Amtsgericht entschied). Die Adressatin der Briefe, ebenso wie die zuständige Kriminalkommissarin und die ebenfalls zuständige Staatsanwältin sahen dies allerdings anders. Die Staatsmacht mobilisierte schwere Geschütze. Sie ging von einem öffentlichen Interesse an der Strafverfolgung aus (üblicherweise werden solche Dinge auf den Privatklageweg verwiesen). Nachdem die wahrscheinliche Identität des Urhebers geklärt war (er hatte in der Hoffnung auf Antwortschreiben sein Postfach als Absenderadresse angegeben), wurde eine Hausdurchsuchung beantragt und richterlich genehmigt, aber nicht durchgeführt.

Die Polizei nahm auch keinen Kontakt zum Verdächtigen auf. Nach drei Monaten (nachdem kein weiteres Verehrerschreiben eingetroffen war) hatte die Polizei wieder Kapazitäten frei und erschien morgens um kurz nach 6 Uhr mit mehreren Beamten im kleinen Haus des Briefeschreibers. Dort überraschte sie – nach dem gewaltsamen Eindringen ins Haus – seine alte behinderte Mutter im Bett des Erdgeschosses, ihn fand sie im Bett des Schlafzimmers des ersten Stocks. Nach einer Durchsuchung des gesamten Hauses (auch des Kellers) wurde – zum Zweck des Schriftvergleichs – ein Notizbuch des Briefeschreibers beschlagnahmt, in dem er Aufzeichnungen über die Krankheit seiner Mutter führte. In seinem Schockzustand widersprach er der Beschlagnahme nicht. Gegen den anschließend von der Staatsanwaltschaft beantragten Strafbefehl über 900 Euro legte er Einspruch ein.

Nach dem amtsgerichtlichen Freispruch aus Rechtsgründen, weil keine Beleidigung vorgelegen hätte, legte die Staatsanwältin Berufung ein. Als das Landgericht die psychiatrische Begutachtung des Briefeschreibers anordnete, wollte dieser lieber nachträglich den Strafbefehl akzeptieren. Es erfolgte eine Einstellung des Verfahrens, wobei der – wirtschaftlich schlecht situierte – Betroffene zur Zahlung der im Strafbefehl genannten Summe und der Kosten verpflichtet wurde.

Die gerichtliche Sicht, dass die drei ursprünglichen Briefe, die Anlass zur Durchsuchung gegeben hatten, im Rahmen des nicht Strafbaren und auch des Hinzunehmenden lagen, wenn die Betroffene als Pressekolumnistin in der Öffentlichkeit steht, entsprach der Einschätzung des LfD. Der Begriff des Stalking erlebt zwar gerade jetzt in der öffentlichen Diskussion eine Blütezeit. Deswegen wird aber nicht schon jede unerwünschte briefliche Annäherung an eine im öffentlichen Leben stehende Person zum Stalkingfall mit kriminellem Unrechtsgehalt.

Vor diesem Hintergrund hatte der LfD – unabhängig von der ihm nicht zustehenden Beurteilung, ob der Durchsuchungsbeschluss im Zeitpunkt seines Erlasses rechtmäßig war – jedenfalls erhebliche Zweifel daran, ob die Vollziehung dieses Beschlusses drei Monate danach und ob die Art und Weise der Vollziehung – am frühen Morgen, als Überraschungsaktion gegenüber den im Bett liegenden und noch schlafenden Bewohnern – verhältnismäßig und damit rechtmäßig war. Hinzu kommt, dass als Schriftprobe ein Notizbuch mit höchstpersönlichen Aufzeichnungen beschlagnahmt wurde. Auch dies hält der LfD für unverhältnismäßig und damit rechtswidrig, unabhängig davon, ob der Betroffene in seinem Zustand der Überraschung und des Schocks dem widersprochen hat oder nicht.

Insgesamt – auch unter weiterer Berücksichtigung der von der Staatsanwaltschaft eingelegten Berufung gegen das freisprechende amtsgerichtliche Urteil – stellen sich für den LfD die angesprochenen Maßnahmen in einem solchen Fall unter dem Gesichtspunkt des Datenschutzes als inadäquat dar.

Da es sich vorliegend sicherlich um einen völlig ungewöhnlichen Einzelfall gehandelt hat, hielt er weitere Erörterungen und Maßnahmen gegenüber der Staatsanwaltschaft nicht für erforderlich. Er hat allerdings ihr gegenüber seine Hoffnung zum Ausdruck gebracht, dass sie in nicht auszuschließenden künftigen vergleichbaren Fällen erwägen sollte, ob nicht die hier vertretene Sicht der Dinge die rechtsstaatlich vorzuziehende wäre.

7.1.3.2 Ist „Einzahlender“ das Gleiche wie „Einzahlungspflichtiger“?

Der Beschwerdeführer hatte für seinen Bruder eine Geldstrafe in die Justizkasse eingezahlt. Daraufhin wurde eine Zahlungsnachricht gefertigt und in die Strafakte seines Bruders aufgenommen, in der er als „Zahlungspflichtiger“ erschien. Dies wurde ihm zufällig bekannt. Er wehrte sich dagegen, dass in der Akte der Eindruck erweckt werde, er sei zu einer Geldstrafe verurteilt und zahlungspflichtig gewesen.

Der LfD konnte dieses Anliegen nachvollziehen. Es gelang ihm, das Ministerium der Justiz davon zu überzeugen, dass damit eine unzutreffende Datenspeicherung erfolgt war. Künftig wird auf solchen Zahlungsanzeigen nur noch eine Kategorie von „Einzahlenden/Einzahlungspflichtigen“ angegeben sein, so dass sich dieses Problem nicht mehr stellen wird.

7.2 Zivilrecht/Registerrecht

7.2.1 Automatisiertes Grundbuchverfahren (elektronisches Grundbuch)

Im 19. Tätigkeitsbericht, Tz. 7.2.1, wurden die Funktion des elektronischen Grundbuchs, die dafür geltende Rechtslage und die aus der Sicht des LfD bestehenden datenschutzrechtlichen Defizite ausführlich dargestellt. Im Berichtszeitraum kündigt sich – wesentlich wohl auch aufgrund der Initiativen der Datenschutzbeauftragten – in diesem Bereich eine positive Entwicklung an. Ein Hauptkritikpunkt am elektronischen Abrufverfahren von Grundbuchdaten war es, dass es die automatisierten Protokolleinträge nicht erlaubten, nachzuvollziehen, welcher Bedienstete einer externen Stelle von welchem Abrufterminal aus auf diese Daten zugegriffen hatte. Nunmehr hat die Justizverwaltung zugesichert, das Verfahren fortentwickeln zu wollen und künftig die aus datenschutzrechtlicher Sicht erforderlichen nutzerbezogenen Zugriffsprotokollierungen zu ermöglichen. Allerdings werden die das Abrufverfahren einsetzenden Stellen (insbesondere die Kommunen) gefordert sein, die entsprechenden programmtechnischen Möglichkeiten zu nutzen und diese technisch-organisatorischen Sicherheitsmaßnahmen auch einzurichten.

Nach wie vor bleibt es ein datenschutzrechtlich nicht zufriedenstellender Zustand, dass es insbesondere den unbeschränkt zugriffsbefugten Stellen (wie den Gemeinden und Notaren) über die Namensabfrage möglich ist, landesweit Erkenntnisse über den Grundbesitz jedes beliebigen Bürgers zu erlangen. Außerdem ist es möglich, unbeschränkt auch Informationen aus den Abteilungen 2 und 3 des Grundbuchs abzurufen. Dies geht selbst aus der Sicht der abrufberechtigten Stellen regelmäßig zu weit. Die umfassende Zugriffsprotokollierung ist zwar ein wichtiges Mittel, um Missbräuchen entgegen zu wirken; ausschließen lassen sich diese damit allerdings nicht. Es bleibt ein wichtiges datenschutzrechtliches Anliegen an den Bundesgesetzgeber, die maßgeblichen Rechtsgrundlagen hier im Sinne einer Beschränkung der Zulässigkeit von online-Zugriffen zu ändern.

Eine Auswertung der vorhandenen Protokollierungen hat ergeben, dass weiterer Prüf- und Korrekturbedarf besteht. So wurde z. B. festgestellt, dass im Auswertungszeitraum Oktober 2003 bis April 2005 ca. 40 % der abrufberechtigten Verwaltungen keine und ca. 30 % weniger als fünf Abrufe getätigt haben. Gemäß § 133 Abs. 2 GBO setzt die Einrichtung eines automatisierten Abrufverfahrens voraus, dass diese Form der Datenübermittlung u. a. unter Berücksichtigung der schutzwürdigen Interessen der betroffenen dinglich Berechtigten wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist. Bei der Beurteilung der Angemessenheit eines derartigen Verfahrens, das mit einer gewissen Gefährdung des Datenschutzgrundrechts einhergeht, sind u. a. die Vorteile für die Verwaltung den möglichen Beeinträchtigungen für die Betroffenen gegenüberzustellen. In vergleichbaren Fällen hat der LfD die Einrichtung eines automatisierten Abrufverfahrens bei einer Zugriffszahl von kleiner als zehn pro Monat für unzulässig gehalten. Ob diese Beurteilung auch für das automatisierte Grundbuch zutrifft, wird mit dem JM noch zu erörtern sein. Außerdem ergaben sich einige Auffälligkeiten im Abrufverhalten einiger angeschlossener Stellen, denen der LfD derzeit nachgeht.

Er bemüht sich weiterhin um eine möglichst datenschutzgerechte Ausgestaltung des Verfahrens. Nach wie vor ist die Bereitschaft des JM positiv hervorzuheben, den LfD umfassend zu informieren und seine Aufgabenerfüllung zu unterstützen.

7.2.2 Automatisiertes Handelsregister

Auch in Rheinland-Pfalz soll das Verfahren RegisStar eingesetzt werden, das in einem Verbund gemeinsam mit zehn anderen Bundesländern entwickelt worden ist und weiter entwickelt wird. Dieses Verfahren ermöglicht zum einen die automatisierte Führung des Handelsregisters, des Vereinsregisters, des Genossenschaftsregisters und des Partnerschaftsregisters. Zum anderen sieht es für die Bürger die Möglichkeit von Abrufen über das Internet vor. Diese können entweder unentgeltlich im örtlichen Amtsgericht oder entgeltlich bei Anmeldung und Zulassung durch die Justizverwaltung vom eigenen Internet-Anschluss aus erfolgen. Ab der ersten Jahreshälfte 2006 soll dieses Verfahren für die Praxis verfügbar sein.

Mit diesem Verfahren sind – wie stets in solchen Fällen – neben erheblichen Vorteilen für alle Nutzer (die Registergerichte und die abfragenden Bürger) auch Risiken verbunden. So ist die Überführung der Altdatenbestände in das automatisierte Register grundsätzlich eine mögliche Fehlerquelle. Der LfD hat Zweifel, ob die vorgesehenen Mechanismen ausreichen, um diese Fehlerquelle zu minimieren. Außerdem bietet der Zugang über das Internet grundsätzlich auch Raum für rechtswidrige Angriffe. Wenn diese Angriffe das System lahmlegen oder – schlimmer noch – zu unbemerkten Datenänderungen führen würden, könnte dies das Wirtschaftsleben empfindlich beeinträchtigen und auch das Datenschutzgrundrecht der Betroffenen verletzen. Der LfD wird vor allem auch unter diesen Aspekten die Entwicklung weiter begleiten.

7.3 Strafvollzug

Eingaben Strafgefangener

Nach wie vor gibt es in den Justizvollzugsanstalten eine ganze Anzahl datenschutzrechtlicher Fragen. Trotz der besonderen gesetzlichen Regelungen dieser Rechtsmaterie im Strafvollzugsgesetz (insbesondere §§ 27, 29, 31, 32, 86, 179 bis 187) finden Strafgefangene nicht selten einen Anlass, um entweder auf Vollzugsdefizite in diesem Bereich oder auf rechtlich ungeklärte Fragen hinzuweisen.

In diesem Zusammenhang hatte sich der LfD beispielsweise mit folgenden Anliegen zu befassen:

Ist es zulässig, dass der Besuchsverkehr in einer JVA mithilfe von Videokameras überwacht wird?

Er kam zu dem Ergebnis, dass es angesichts der bestehenden Personalknappheit in den Justizvollzugsanstalten im Interesse einer uneingeschränkten Besuchshäufigkeit einerseits, eines akzeptablen Sicherheitsstandards andererseits vertretbar ist, auch Videokameras einzusetzen, wenn gewährleistet ist, dass die Aufzeichnungen kurzfristig (innerhalb von spätestens 48 Stunden) gelöscht werden und wenn die Auswertungen dieser Aufnahmen nur anlassbezogen kontrolliert erfolgen können. § 27 Abs. 1 i. V. m. §§ 179 Abs. 1 und 180 Abs. 1 StrVollzG bietet hierfür eine Rechtsgrundlage.

Dürfen im Warteraum die Besucher namentlich aufgerufen werden – mit der Folge, dass die Mitwartenden die Namen erfahren?

Der LfD vertritt die Auffassung – nunmehr in Übereinstimmung mit der betroffenen JVA –, dass diese Verfahrensweise nicht erforderlich und damit unzulässig ist. Die JVA hat auf ein Nummernsystem umgestellt.

Dürfen im Rahmen des Anstaltseinkaufs Mitgefangene die Konsumgewohnheiten und den Kontostand der Häftlinge erfahren?

Hierzu sind die Erörterungen mit der betroffenen JVA derzeit noch nicht abgeschlossen.

Ist eine bestimmte JVA zu hellhörig gebaut? Können Mitgefangene deshalb Gespräche des Vollzugspersonals mit den Häftlingen mithören?

Auch diese Fragen sind derzeit noch nicht abschließend geklärt.

Unter welchen Voraussetzungen darf die JVA den Gläubiger eines Gefangenen über dessen Entlassdatum unterrichten?

Die hierfür geltenden Voraussetzungen sind im StVollzG detailliert geregelt. § 180 Abs. 5 StVollzG bestimmt, dass nicht-öffentlichen Stellen die Vollzugsbehörde auf schriftlichen Antrag mitteilen darf, ob sich eine Person in Haft befindet sowie ob und wann ihre Entlassung voraussichtlich innerhalb eines Jahres bevorsteht, soweit ein berechtigtes Interesse an dieser Mitteilung glaubhaft dargelegt wird und der Gefangene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.
Im konkreten Fall lag bei der Auskunftserteilung durch die JVA weder ein schriftlicher Antrag vor, noch lag der Entlassungszeitpunkt innerhalb eines Jahres nach der Anfrage. Die JVA sicherte zu, die gesetzlichen Vorgaben künftig zu beachten.

Werden bei der Ausgabe der Post und von Medikamenten andere Gefangene (die Hausarbeiter) unzulässigerweise über persönliche Angelegenheiten ihrer Mitgefangenen unterrichtet?

Es ergab sich, dass die Befürchtungen des Gefangenen unbegründet waren.

Werden die in der anstaltseigenen Datei gespeicherten digitalen Fotos der Gefangenen entsprechend den gesetzlichen Vorgaben nur eingeschränkt und zweckgebunden genutzt, oder ist es zu weitgehend, dass jeder Stationsbeamte hierauf Zugriff hat?

Die JVA konnte die Notwendigkeit dieser Datennutzungen überzeugend begründen.

Werden den Vollzugsbeamten beim Arztbesuch unzulässigerweise Gesundheitsdaten offenbart?

Auch hier haben sich die Befürchtungen des Gefangenen nicht bestätigt.

Durfte die Mutter eines Gefangenen über bestimmte Erkenntnisse der JVA unterrichtet werden?

Es ergab sich kein Hinweis auf unzulässiges Verhalten von Bediensteten der JVA.

Dürfen Hausarbeiter beim Einsammeln der Post mithelfen?

Grundsätzlich dürfen Hausarbeiter nicht erfahren, wer mit wem korrespondiert. Dies wird in den Anstalten durch den Einsatz mobiler Briefkästen verhindert, in die die Hausarbeiter keinen Einblick nehmen können. Auch für größere Postsendungen sind Vorkehrungen zu treffen, die das verhindern.

Immer wieder wird problematisiert, ob die Namensschilder an den Zellen beim Einsatz anstaltsfremder Personen, z. B. externer Techniker oder Handwerker, abgedeckt werden müssen. Hier kollidiert das ausgeprägte Datenschutzbewusstsein einiger Gefangener mit den praktischen Schwierigkeiten bei der Umsetzung des datenschutzrechtlich Geforderten.

In welchem Umfang können Gefangene aus ihrer Personalakte Kopien beanspruchen?

Hier haben die Anstalten einen Ermessensspielraum. Der LfD hat keine Beanstandung ausgesprochen.

Ist das Wahlgeheimnis bei der Briefwahl Gefangener gewahrt?

Die Überprüfung durch den LfD ergab, dass hier keine Defizite bestanden.

Besonders spektakulär war der Fall eines Vollzugsbediensteten, der die (wahrscheinlich besonders reizvolle) Freundin eines Gefangenen dadurch – telefonisch – zu näheren Kontakten zu nötigen versuchte, dass er vorgab, er könne ihren inhaftierten Freund besser oder schlechter behandeln, je nachdem, wie entgegenkommend sie sich verhalte. Datenschutzrechtlich gesehen hat hier eine zweckwidrige Nutzung dienstlich erlangter Daten (insbesondere auch der Anschrift und der Telefonnummer der Freundin) vorgelegen. Dieser Aspekt wurde bei der folgenden straf- und disziplinarrechtlichen Ahndung allerdings aus der Sicht des LfD nicht genügend berücksichtigt.

Das Verfahren beim Telefonieren Gefangener und die Frage der dafür zulässigen Aufsicht durch die JVA hat ebenfalls wieder eine Rolle gespielt. Fraglich war auch, ob die Vorkehrungen ausreichend sind, dass andere Gefangene keine Einsicht in die zu führenden Telefonlisten nehmen können. Auch der Aufenthalt anderer Gefangener an der Telefonzelle während des Telefonierens wurde gerügt. Es gab allerdings keinen Anlass für eine Beanstandung.

Die Nutzung des Gefangenen-Personalbogens, des sog. „A-Bogens“ für die Unterrichtung anderer Stellen (z. B. des Arbeitsamtes bei Vermittlungsmaßnahmen oder der Polizei bei Aufnahme in die JVA) war erneut Gegenstand der Diskussion. Diese Verfahrensweise ist zwar für die Verwaltung der JVA einfach, sie geht aber regelmäßig mit der Übermittlung nicht erforderlicher Informationen (z. B. über die Religionszugehörigkeit oder die Kinderzahl) einher. Hier konnte bezüglich der künftig zu beachtenden Verfahrensweise Einvernehmen mit dem JM erzielt werden.

Gegenstand einer Eingabe war schließlich die Frage, ob die Hausarbeiter, die in der Bibliothek helfen, wirklich das Geburtsdatum ihrer lesewilligen Mitgefangenen bei der Ausleihe brauchen, um sie identifizieren zu können, oder ob nicht andere Möglichkeiten bestehen. Die betroffene JVA will aufgrund der an sie herangetragenen Eingabe zunächst probeweise ihr Entleihsystem so umstellen, dass sie auf die Erfassung des Geburtsdatums verzichtet.

7.4 Sonstiges

7.4.1 Internet-Veröffentlichungen von Rechtsanwaltskammern

Aufgrund einer Eingabe hatte der LfD sich mit folgender Frage zu befassen:
Der Beschwerdeführer war ein Anwalt, für den zunächst ein amtlich bestellter Vertreter ernannt wurde, weil die Anwaltskammer wegen des Verdachts des Vermögensverfalls ein vorläufiges Tätigkeitsverbot ausgesprochen hatte. Diese Vertreterbestellung wurde in den Kammernachrichten – einem monatlich erscheinenden Veröffentlichungsorgan der Kammer – publiziert. Diese Kammernachrichten sind außerdem im Internet unbeschränkt abrufbar.

Nachdem der Anwalt die Rücknahme der gegen ihn verhängten Maßnahme erreichen konnte, wurde er ca. ein Jahr später tatsächlich zahlungsunfähig – nach seinem Vortrag wegen der ursprünglich gegen ihn erlassenen seiner Ansicht nach unrechtmäßigen Maßnahmen, die zu einem Abwandern seiner Mandanten geführt hätten. Auch die Rückgabe seiner Anwaltszulassung wurde in gleicher

Weise publiziert. Er sucht nun eine Beschäftigung als Arbeitnehmer und erklärt, die unbeschränkte Veröffentlichung der ihn betreffenden Daten in den Kammernachrichten ermöglichten es jedem potentiellen Arbeitgeber, Informationen über das Internet abzurufen, die ihn von vornherein diskriminieren würden.

Tatsächlich ist es so, dass bei Eingabe des – ungewöhnlichen – Namens des Betroffenen in eine Internet-Suchmaschine sofort die fraglichen Einträge in den Kammernachrichten auftauchen.

Der LfD hatte in der Vergangenheit vertreten, dass wegen dieser leichten, umfassenden und unbeschränkten Recherchemöglichkeiten die Veröffentlichungen öffentlicher Stellen nur dann auch im Internet erfolgen dürfen, wenn dies entweder gesetzlich ausdrücklich vorgeschrieben ist oder wenn die Betroffenen eingewilligt haben.

Ob dieser Grundsatz auch im vorliegenden Zusammenhang gilt, wird derzeit noch zwischen den betroffenen Stellen erörtert.

7.4.2 Zur Zustellung/Übersendung von Schriftstücken

Im Zusammenhang mit der Zustellung bzw. der Übersendung von Schriftstücken kommt es immer wieder zu Datenschutzverstößen. So wurde ein Betreuer von der Justizkasse im Adressenfeld eines Schreibens ausdrücklich als Betreuer einer bestimmten namentlich genannten Person bezeichnet. Dies führte zu einer unzulässigen Informationsübermittlung an alle diejenigen Personen, die mit der Übermittlung des Briefes an den Adressaten befasst waren (unter Einschluss des Zustellers). Es wurden seitens der Justiz Vorkehrungen getroffen, die dies künftig verhindern sollen.

In einem anderen Fall wurde ein Schreiben an einen falschen Adressaten gesandt. Hierbei handelte es sich um ein Versehen. Organisatorische Änderungen waren nicht veranlasst.

Schließlich sandte ein Gericht in einem sozialgerichtlichen Verfahren ungeprüft alle Unterlagen, die eine Partei vorgelegt hatte, an die Gegenpartei. Bei diesen Unterlagen befand sich das sozialgerichtliche Urteil eines anderen Verfahrens, in dem die Krankheiten und der Gesundheitszustand eines an dem laufenden Verfahren völlig Unbeteiligten detailliert dargelegt worden waren. Dieses Urteil sollte die Rechtsauffassung der übersendenden Partei stützen; eine anonymisierte Fassung hätte diesen Zweck in völlig gleicher Weise erfüllt. Obwohl der Hauptvorwurf in diesem Fall der übersendenden Partei zu machen war, so hat doch das Sozialgericht anerkannt, in solchen Fällen auch eine eigene Überprüfungspflicht zu haben. Es hat erklärt, darauf künftig achten zu wollen.

Zunehmend werden private Postdienstleister mit der Zustellung gerichtlicher Postsendungen betraut. Dies nahm der LfD zum Anlass, darauf hinzuweisen, dass aus seiner Sicht mit diesen Postdienstleistern vertraglich zu vereinbaren ist, dass der LfD auch ihnen gegenüber ein Kontrollrecht besitzt (§ 4 LDSG). Das JM prüft derzeit noch, ob es sich dieser Auffassung anschließen kann.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 Neues Schulgesetz

Seit 1. August 2004 gilt das neue Schulgesetz vom 30. März 2004. In diesem ist die Datenverarbeitung in der Schule nunmehr in § 67 geregelt. Dort werden folgende Fälle unterschieden:

- Datenverarbeitung innerhalb der Schule (Abs. 1)
- Evaluationen (Abs. 2)
- Lehreraus- und -fortbildung, Qualitätsentwicklung (Abs. 3)
- Datenübermittlung an andere öffentliche Stellen (Abs. 4)
- Datenübermittlung an Private (Abs. 5)
- Datenverarbeitung für wissenschaftliche Untersuchungen (Abs. 6)
- Statistik (Abs. 8).

Im Gegensatz zur bisherigen Regelung wurden jetzt die Evaluationen durch die Schulbehörden, die Maßnahmen im Rahmen der Lehreraus- und -fortbildung und Qualitätsentwicklung sowie die Datenverarbeitung für wissenschaftliche Untersuchungen auf eigene gesetzliche Grundlagen gestellt. Diese Differenzierung wird den unterschiedlichen datenschutzrechtlichen Anforderungen der einzelnen Datenverarbeitungsvorgänge gerecht und schafft zudem Rechtssicherheit bei den Betroffenen. Die Handreichung für den schulischen Datenschutzbeauftragten im Internet-Angebot des LfD wurde den neuen Regelungen angepasst.

8.1.2 Befragungen in Schulen

Im Berichtszeitraum war der LfD wieder gefordert, eine Vielzahl von geplanten Befragungen im Schulbereich zu begutachten. Studierende nutzen oft den Kreis von Schülerinnen und Schülern, Eltern und Lehrerinnen und Lehrern, um für ihre Abschlussarbeiten relevante Daten zu erhalten. Hierbei stellt sich stets als erstes die Frage, ob die Befragung anonym oder doch zumindest personenbeziehbar durchgeführt werden soll. Viele der Anfragenden gehen von einer Anonymität aus, da sie keine Namen der Betroffenen

erheben. Dabei wird oft nicht berücksichtigt, dass aus der Kombination anderer Informationen ohne unverhältnismäßig großen Aufwand auf die Person der Antwortenden geschlossen werden könnte. Die Wahrscheinlichkeit der Personenbeziehbarkeit ist um so größer, je kleiner der Kreis der Befragten ist. Wenn dann z. B. nach dem Wohnort eines Schülers und dem Beruf der Mutter gefragt wird und die Mutter zufällig Bürgermeisterin im Ort ist, ist der antwortende Schüler auch für Schulfremde einfach zu identifizieren. Werden solche personenbezogenen oder personenbeziehbaren Daten in der Schule für wissenschaftliche Untersuchungen erhoben, setzt dies gem. § 67 Abs. 6 SchulG die Genehmigung der Schulbehörde (Aufgabe wurde der ADD übertragen) und die Einwilligung der Betroffenen voraus. Diese sind wiederum gem. § 5 Abs. 2 LDSG in geeigneter Weise über die Bedeutung der Einwilligung, den vorgesehenen Zweck der Verarbeitung, den möglichen Empfängerkreis sowie die verantwortliche Stelle aufzuklären. Sind die Schülerinnen und Schüler noch sehr jung und die Fragen sensibel, ist auch die Einwilligung der Eltern einzuholen. Besondere Anforderungen sind zu stellen, wenn besondere Arten personenbezogener Daten verarbeitet werden sollen. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 3 Abs. 9 LDSG). So sollte eine Umfrage zum Thema „Politiklust oder Politikfrust?“ durchgeführt werden. Ebenso interessierte man sich in einem anderen Vorhaben für die „Verbreitung okkultistischer und satanistischer Kenntnisse bei Jugendlichen“. In diesen Fällen muss sich die Einwilligung ausdrücklich auf diese besonderen Arten personenbezogener Daten beziehen (§ 5 Abs. 4 LDSG). Stets ist die Freiwilligkeit der Teilnahme zu betonen. Viele holen zwar die Einwilligung der Eltern in Schülerbefragungen ein, vergessen aber oftmals, auch die Schüler selbst zu informieren und auf die Freiwilligkeit hinzuweisen. Denn selbst wenn die Eltern nichts gegen eine Teilnahme ihrer Kinder haben, behalten diese das letzte Wort. Sie können zum Mitmachen nicht gezwungen werden. Oftmals sollen die Lehrer die Fragebögen einsammeln. Diese könnten sich dann leicht einen Überblick verschaffen, welcher ihrer Schüler welche Antwort gegeben hat. Um dies zu vermeiden, sollte die Rückgabe ohne die Möglichkeit der Kenntnisnahme von Lehrern organisiert werden. So erschweren z. B. ein verschlossener Umschlag oder eine Urne den unberechtigten Zugang.

Wenn also die Betroffenen hinreichend über die geplante Erhebung personenbezogener oder personenbeziehbarer Daten und die Freiwilligkeit ihrer Teilnahme informiert worden sind und auf dieser Grundlage eingewilligt haben, stehen der Durchführung solcher Befragungen durch Dritte an der Schule grundsätzlich keine datenschutzrechtlichen Bedenken entgegen.

Eine eigene Rechtsgrundlage haben mit der Neufassung des Schulgesetzes im August 2004 auch die externen Schulevaluationen durch die Schulbehörden gefunden. Nach § 67 Abs. 2 SchulG können die Schulbehörden zu Zwecken der Evaluation geeignete Verfahren einsetzen und durch Befragungen und Unterrichtsbeobachtungen erhobene Daten verarbeiten. Die Betroffenen müssen vorab über das Ziel des Vorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung ihrer Daten informiert werden. Personenbezogene Daten für diese Zwecke dürfen ohne Einwilligung der Betroffenen verarbeitet werden, wenn das öffentliche Interesse an der Durchführung eines von der Schulbehörde genehmigten Vorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Schulinterne Evaluationen hingegen können auf § 67 Abs. 1 SchulG gestützt werden. Danach sind Schüler, Eltern und Lehrer zur Angabe ihrer Daten verpflichtet, wenn dies für die Erfüllung einer schulbezogenen Aufgabe erforderlich ist. Die unterschiedlichen Voraussetzungen für interne und externe Evaluationen lassen sich dadurch rechtfertigen, dass der Kreis der Datenverarbeiter innerhalb der Schule wesentlich kleiner und vertrauter ist als bei einer Datenerhebung von außen.

Schließlich ist nunmehr auch ausdrücklich festgelegt, unter welchen Voraussetzungen im Rahmen der Lehrerausbildung und -fortbildung und der Qualitätsentwicklung von Unterricht Bild- und Tonaufzeichnungen des Unterricht erfolgen dürfen (§ 67 Abs. 3 SchulG). Die Betroffenen sind rechtzeitig über die beabsichtigten Maßnahmen zu informieren und können diesen widersprechen. Eine Löschung der Aufnahmen ist spätestens nach fünf Jahren vorgeschrieben.

8.1.3 Mehr Rechte für Eltern – Bestätigung durch den Verfassungsgerichtshof

Im 19. Tb. (Tz. 8.1.2) wurde über die neue Regelung im Schulgesetz berichtet, wonach die Schule unter bestimmten Voraussetzungen die Eltern volljähriger Schüler unterrichten darf. Dies stellt zwar eine Einschränkung des informationellen Selbstbestimmungsrechts von Schülern dar. Dennoch wurde die Regelung vom LfD mitgetragen, u. a. deshalb, weil Ausnahmen von der Unterrichtungspflicht vorgesehen sind und somit schutzwürdige Belange betroffener Schüler berücksichtigt werden können. Die Verfassungsbeschwerde einer volljährigen Schülerin gegen diese Regelung wies der Verfassungsgerichtshof mit Urteil vom 22. Juni 2004 zurück. In den Leitsätzen des Urteils heißt es:

„Die Verfassung für Rheinland-Pfalz (LV) steht einer Regelung nicht entgegen, wonach die Eltern auch volljähriger Schüler über schwerwiegende schulische Vorkommnisse unterrichtet werden sollen, um das Risiko von Selbst- und Fremdgefährdungen zu vermindern. Der hierdurch bewirkte Eingriff in das Recht auf Selbstbestimmung über personenbezogene Daten (Art. 4 a LV) ist aus überwiegenden Interessen der Allgemeinheit gerechtfertigt. Der Gesetzgeber hat hinreichend Vorsorge dafür getroffen, dass in Fällen, in denen sich die Unterrichtung der Eltern als untaugliches Mittel für eine vorteilhafte Einflussnahme auf den Schüler erweist, ein dann unverhältnismäßiger Eingriff in das Grundrecht vermieden wird.“

8.1.4 Schulstatistik

Nach § 67 Abs. 8 SchulG sind die Schulen verpflichtet, den Schulbehörden, den Schulträgern und dem Statistischen Landesamt erforderliche Einzelangaben über Schüler und Lehrer zu übermitteln. Dabei dürfen Name, Geburtstag, Adresse und Personalnummer nicht an das Statistische Landesamt und die Schulträger übermittelt werden.

Im Berichtszeitraum erfolgte die Datenübermittlung in der Weise, dass die Schulen alle erforderlichen Einzelangaben einschließlich Name, Geburtstag, Adresse und Personalnummer an das Statistische Landesamt übermittelten. Dort wurden die Daten weiter verteilt: Die Schulbehörden erhielten die für sie bestimmten Datensätze. Das Statistische Landesamt selbst griff nicht auf die genannten Personenkennzeichen zu, sondern filterte nur die für seine Arbeit erforderlichen Daten heraus.

Durch dieses Verfahren entstand der Eindruck, dass im Widerspruch zum Gesetzestext personenbezogene Daten an das Statistische Landesamt übermittelt wurden. Der LfD prüfte diese Frage und kam zur Auffassung, dass dies nicht zutraf. Unter dem Dach des Statistischen Landesamtes werden sowohl ein Rechenzentrum als auch das Statistische Landesamt betrieben. Das Rechenzentrum nimmt auch für andere öffentliche Stellen des Landes Datenverarbeitungsaufgaben wahr, die unabhängig vom Statistikbereich sind. So war es auch im vorliegenden Fall: Die Datenverteilung durch das Rechenzentrum war unabhängig von der Erstellung der Schulstatistik. Auch wenn der Anschein erweckt wurde, die Daten würden an das Statistische Landesamt übermittelt, kamen sie doch bei dem davon getrennten Rechenzentrum an. Der LfD hatte daher grundsätzlich keine datenschutzrechtlichen Bedenken gegen das bestehende Übermittlungsverfahren. Er empfahl jedoch, dieses gegenüber den Schulen transparent zu gestalten.

8.1.5 Schüler bewerten Lehrer

Ein Lehrer an einer berufsbildenden Schule hatte ohne Wissen der Schulleitung und der Kollegen von Schülern die Fachlehrer zweier Technikerklassen bewerten lassen. Die Ergebnisse präsentierte er in der Schule. Die Kollegen mit besonders guten Ergebnissen wurden farblich hervorgehoben. Daraufhin beschwerte sich ein betroffener Lehrer der Schule beim LfD über das Vorgehen seines Kollegen, u. a. auch weil er keine Auskunft über seine „Ergebnisse“ erhalten konnte.

Durch die Evaluation wurden personenbezogene Daten innerhalb der Schule erhoben und verarbeitet. Da dies vor In-Kraft-Treten des neuen Schulgesetzes (vgl. Tz. 8.1.1) erfolgte, richtet sich die Zulässigkeit des Datenverarbeitungsvorganges nach § 54 a Abs. 1 Schulgesetz (vom 6. November 1974, gültig bis 31. Juli 2004). Danach durften personenbezogene Daten von Lehrern innerhalb der Schule verarbeitet werden, soweit dies zur Erfüllung der der Schule durch Rechtsvorschrift zugewiesenen Aufgabenerfüllung erforderlich war. Die Evaluation und damit Qualitätssicherung und auch -verbesserung ist eine der Schule obliegende Aufgabe. Hierbei ist die Befragung von Schülern zum Unterrichtsverhalten von Lehrern eine von vielen Möglichkeiten, so dass diese Art der Evaluation grundsätzlich datenschutzrechtlich zulässig war.

Jedoch war ein für die Betroffenen transparentes Verfahren einzuhalten: Das Landesdatenschutzgesetz sieht vor, dass die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten von der verantwortlichen Stelle unterrichtet werden (§ 18 Abs. 1 LDSG). Nur wer von der Datenverarbeitung weiß, kann auch seine Auskunftsrechte geltend machen. Hier wurde erst nach Abschluss der Evaluation über die Datenverarbeitung unterrichtet.

Den Betroffenen stand auch unabhängig von der datenschutzgerechten Ausgestaltung der Evaluation ein Auskunftsrecht zu, zumal der seit 1. August 2004 geltende § 67 Abs. 2 SchulG ausdrücklich vorsieht, dass die Betroffenen vorab über das Ziel der Evaluation, die Art ihrer Beteiligung an der Untersuchung sowie die Datenverarbeitung informiert werden. Im vorliegenden Fall konnte die Auskunft jedoch nicht mehr erteilt werden, da der Schulleiter unmittelbar, nachdem er von der Aktion erfahren hatte, die sofortige Vernichtung der Unterlagen anordnete.

8.1.6 Videoüberwachung an Schulen

Die Videoüberwachung an Schulen hat den LfD auch in diesem Berichtszeitraum wieder beschäftigt (vgl. hierzu auch 19. Tb., Tz. 8.1.4). Angefacht wurde die Diskussion durch Medienberichte über sexuelle Übergriffe an Schulen, insbesondere den Überfall auf ein Mädchen auf der Schultoilette an einer Koblenzer Grundschule Ende 2003. Dies führte bei vielen Schulen, Schulträgern und der Aufsichtsbehörde zu Überlegungen, wie die Sicherheit an Schulen erhöht werden kann. Dabei wurden auch die Möglichkeiten der Videoüberwachung diskutiert.

Eine solche Videoüberwachung ist nach § 34 LDSG zu beurteilen. Sie ist zulässig, soweit dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Eine Videoüberwachung zur Gewährleistung der größtmöglichen Sicherheit der Schülerinnen und Schüler dient der Ausübung des Hausrechts. Es soll dadurch gewährleistet werden, dass nur solche Personen das Schulgelände betreten, die hierzu berechtigt sind, und dass diese Personen sich rechtmäßig verhalten. Will man nur verhindern, dass Unberechtigte auf das Schulgelände gelangen, ist sicherlich eine Videoüberwachung ohne Aufzeichnung die geeignete Methode. Dabei muss sichergestellt sein, dass der Übertragungsmonitor ununterbrochen beaufsichtigt wird. Eine Aufzeichnung kann dagegen in diesem Fall den gewünschten Zweck nicht erfüllen, da sie nicht zu einer unmittelbaren Reaktion führen kann. Sie wäre damit aus datenschutzrechtlicher Sicht unzulässig, da sie zur Zweckerreichung nicht erforderlich ist. Ist beabsichtigt, rechtswidrige Handlungen auf dem Schulgelände aufzuklären, kommt auch eine Videoaufzeichnung in Betracht. Voraussetzung ist jedoch, dass insoweit ein deutlicher Verdacht besteht. Dies ist immer dann der Fall, wenn es bereits in der Vergangenheit zu rechtswidrigen Handlungen gekommen ist. Dann kann eine Videoüberwachung mit Aufzeichnung als erforderlich angesehen werden. In beiden Fällen sind die weiteren Voraussetzungen des § 34 LDSG zu beachten: Kenntlichmachung der Maßnahme, Auswertung nur bei Erforderlichkeit, evtl. Information des Betroffenen und Löschung, wenn die Daten nicht mehr erforderlich sind.

8.1.7 Was gehört ins Klassenbuch?

Fragen nach dem zulässigen Inhalt des Klassenbuchs erreichen den LfD sehr häufig, sowohl aus der Lehrerschaft als auch von den Eltern. Die zulässigen Eintragungen in das Klassenbuch sind in den verschiedenen Schulordnungen abschließend geregelt. Als Beispiel sei § 76 Abs. 5 der Schulordnung für die öffentlichen Hauptschulen, Regionalen Schulen, Realschulen, Gymnasien, Integrierte Gesamtschulen und Kollegs (Übergreifende Schulordnung) genannt. Danach dürfen im Klassenbuch stehen:

- Namen und Geburtsdatum der Schüler,
- Teilnahme an Schulveranstaltungen,
- Vermerk über unentschuldigtes und entschuldigtes Fernbleiben und über Beurlaubungen,
- erzieherische Einwirkungen gem. § 83 Abs. 1,
- Namen und Anschrift der Eltern,
- Angaben zur Herstellung des Kontakts in Notfällen.

Eltern beschwerten sich über einen Eintrag ins Klassenbuch, wonach ihr Kind einem anderen ein Mäppchen entwendet und beschädigt haben soll. Es hatte, so war dem Eintrag weiter zu entnehmen, zur Wiedergutmachung einen Kleinstbetrag geleistet. Die Eltern sahen ihr Kind durch den entsprechenden Klassenbucheintrag als Dieb gebrandmarkt, obwohl die Handlung im Gerangel mit mehreren und ohne Absicht erfolgt sei.

Bei dem Eintrag handelte es sich um das Festhalten einer erzieherischen Einwirkung gem. § 83 Abs. 1 Übergreifende Schulordnung. Danach kommen als erzieherische Einwirkungen insbesondere in Betracht: Gespräch, Tadel, Verpflichtung zur Wiedergutmachung angerichteten Schadens, Nacharbeiten von Versäumtem, Entschuldigung für zugefügtes Unrecht und Überweisung in eine andere Klasse oder in einen anderen Kurs derselben Klassen- oder Jahrgangsstufe der Schule. Der fragliche Eintrag schilderte das Verhalten des Kindes und die damit verbundene erzieherische Einwirkung, nämlich die Wiedergutmachung angerichteten Schadens. Ein solcher Eintrag ist gem. § 76 Abs. 5 Nr. 4 Übergreifende Schulordnung zulässig. Der zugrundeliegende Sachverhalt war unstreitig: Der Schüler hatte einer Mitschülerin das Mäppchen vom Tisch weggenommen und auf einen anderen Tisch gelegt, von wo Dritte es an sich genommen und beschädigt haben. Es ist auch aus datenschutzrechtlicher Sicht vertretbar, diesen Vorgang so zusammenzufassen, wie es die Klassenlehrerin in ihrem Klassenbucheintrag getan hatte. Das Entfernen eines Gegenstands aus dem Zugriffsbereich des Berechtigten gegen dessen ausdrücklich geäußerten oder auch nur zu vermutenden Willen kann zutreffender- und zulässigerweise mit dem Begriff „entwenden“ bezeichnet werden. Das Vorgehen der Schule war daher datenschutzrechtlich nicht zu beanstanden.

8.1.8 Homepage einer Schule und Datenschutz

Die Frage, ob und welche personenbezogenen Daten auf der Homepage einer Schule veröffentlicht werden dürfen, hat den LfD auch in diesem Berichtszeitraum beschäftigt. Die Rechtslage ist eindeutig (vgl. 18. Tb., Tz. 8.1.4 und 17. Tb., Tz. 8.1.7): Vor der Veröffentlichung personenbezogener Daten im Internet durch eine Schule ist grundsätzlich das Einverständnis der Betroffenen hierzu einzuholen. Das gebietet das Recht auf informationelle Selbstbestimmung. Dieses Recht ist jedoch dann eingeschränkt, wenn der Betroffene ein Amt ausübt und in dieser Funktion die Schule auch nach außen vertritt. Über die Veröffentlichung von Daten, die ihn in dieser Funktion beschreiben, kann er nicht selbst bestimmen und hat daher in der Regel eine Veröffentlichung von Name, Funktion und Erreichbarkeit hinzunehmen. Dies betrifft z. B. den Schulleiter, den Schülersprecher oder auch den Schulelternsprecher. Ein stellvertretendes Mitglied des Schulelternbeirates ist jedoch nicht als ein solcher Funktionsträger zu bewerten.

Bei einigen Schulen besteht in dieser Hinsicht noch erhebliche Rechtsunsicherheit, wie zahlreiche Anfragen belegen. Daher wird auch in Fortbildungsveranstaltungen versucht, diese Voraussetzungen zu vermitteln.

8.1.9 Elternbriefe als E-Mail

Eine Schule plante, Elternbriefe per E-Mail zu verschicken. Hierbei ist Folgendes zu beachten:

Sollen Elternbriefe, die an alle Eltern mit den gleichen allgemeinen Schulinformationen verteilt werden, per E-Mail verschickt werden, bestehen hiergegen grundsätzlich keine datenschutzrechtlichen Bedenken.

Soll dagegen der individuelle Kontakt mit den Eltern auf diesem Weg erfolgen (z. B. die Benachrichtigung über das Verhalten oder über Noten des Kindes), sind Maßnahmen zu treffen, die vor Kenntnisnahme der personenbezogenen Daten durch Dritte schützen (z. B. Verschlüsselung). Auch der Austausch personenbezogener Daten mit anderen Stellen wie z. B. der Aufsichts- und Dienstleistungsdirektion erfolgt über EPOS (Elektronische Post für Schulleitungen), also auf einem geschützten Weg.
In allen Fällen ist es aber erforderlich, dass die Eltern gegenüber der Schule ihre E-Mailadresse angeben. Hierbei ist darauf hinzuweisen, dass die Angabe freiwillig ist und die Informationen auch auf „herkömmlichem“ Weg bezogen werden können. Zudem sollte das Einverständnis für den Versand von individuellen Informationen per E-Mail eingeholt werden, auch um sicherzustellen, dass die Eltern hiervon Kenntnis nehmen werden.

8.2 Hochschulen

8.2.1 BAföG-Empfänger im Visier

Das Bundesamt für Finanzen ist gem. § 45 d Abs. 2 EStG berechtigt, den Sozialleistungsträgern, also auch dem Amt für Ausbildungsförderung, Name, Geburtsdatum und Anschrift des Auftraggebers eines Freistellungsauftrages sowie die freigestellte Summe mitzuteilen, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist oder der Betroffene zustimmt. § 41 Abs. 4 BAföG ermächtigt die Ämter für Ausbildungsförderung Personen, die Leistungen nach dem BAföG beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und welche Daten nach § 45 d Abs. 1 EStG dem Bundesamt für Finanzen übermittelt worden sind. § 41 Abs. 4 BAföG ermächtigt die Ämter für Ausbildungsförderung zu diesem Zweck Namen, Geburtsdatum und Anschrift der Leistungsempfänger an das Bundesamt für Finanzen zu übermitteln. Die gesetzlichen Grundlagen beschränken den Datenabgleich auch dann nicht, wenn eine bestimmte Summe im Freistellungsauftrag nicht überschritten wird.

Die Länder haben sich jedoch darauf verständigt, Ermittlungen nur in solchen Fällen aufzunehmen, in denen der Betrag 100,– € übersteigt. In einigen Fällen wurde von dieser Verfahrensweise abgewichen. Dabei handelte es sich, wie sich auf Nachfrage beim MWWFK herausstellte, nicht um willkürlich herausgegriffene Fälle, sondern um einen Irrtum. Dieser beruht darauf, dass in der Abfrageoption lediglich die Zahl „100“ ohne Währungsangabe eingegeben wurde, das System aber 100,– DM statt 100,– € als Auswahlkriterium nutzte. Da die gesetzliche Grundlage nicht auf einen Mindestbetrag abstellt und die Verfahren teilweise schon eingeleitet waren, konnte in diesen Fällen nicht mehr von einer Verfolgung abgesehen werden. Dies war zwar unbefriedigend für die Betroffenen, die sich schlechter gestellt sahen als andere. Datenschutzrechtlich war das Vorgehen jedoch nicht zu beanstanden.

8.2.2 BAföG-Akte beim Justitiar

Ein Studierender hatte beim Amt für Ausbildungsförderung an einer Hochschule einen Antrag auf BAföG-Förderung gestellt, bei dessen Bearbeitung es zu Problemen gekommen war. Die Auszahlung hatte sich dadurch verzögert. Aufgrund der Beschwerde des Betroffenen hatte das Amt für Ausbildungsförderung die Förderungsakte an den Justitiar der Hochschule weitergeleitet. Dieser hatte die Angelegenheit sodann gegenüber dem Studierenden rechtlich beurteilt. Dieser hielt die Übermittlung seiner Förderungsakte für datenschutzrechtlich unzulässig.

Das Amt für Ausbildungsförderung nimmt gem. § 41 Abs. 1 Satz 1 BAföG die zur Durchführung des BAföG erforderlichen Aufgaben wahr. Die dabei verarbeiteten Daten sind Sozialdaten im Sinne von § 67 Abs. 1 SGB X. Eine Übermittlung solcher Sozialdaten ist gem. § 69 Abs. 1 Nr. 1 SGB X zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch erforderlich ist. Aufgabe des Amtes für Ausbildungsförderung ist, wie bereits dargestellt, die Bearbeitung von BAföG-Anträgen. Kommt es in diesem Zusammenhang zu rechtlichen Schwierigkeiten oder auch Beschwerden des Antragstellers, sind diese ebenfalls zu bearbeiten. Verfügt das Amt für Ausbildungsförderung selbst nicht über geeignete Kapazitäten, kann es sich eines dritten Rechtskundigen bedienen. § 41 Abs. 1 Satz 2 BAföG ermöglicht ausdrücklich bei der Bearbeitung der Anträge die Heranziehung von zentralen Verwaltungsstellen. Das Amt für Ausbildungsförderung hatte sich entsprechend verhalten: Es hat den Justitiar der Hochschule mit der rechtlichen Bearbeitung der Beschwerde betraut. Die Übermittlung der Förderungsakte an diesen war daher gem. § 69 Abs. 1 Nr. 1 SGB X zulässig.

8.2.3 Krank zur Prüfung

Mit der Frage der datenschutzrechtlichen Bewertung der Anforderungen an Atteste wegen Prüfungsunfähigkeit hatte sich der LfD aufgrund der Nachfragen von Hochschulen, Studierenden und auch Ärzten in der Vergangenheit immer wieder zu beschäftigen (vgl. 14. Tb., Tz. 8.2.3). Viele Betroffene sehen das Arztgeheimnis verletzt, wenn das Prüfungsamt genauere Angaben zum Krankheitsverlauf fordert und sich nicht lediglich mit der Feststellung des Arztes „prüfungsunfähig“ zufrieden gibt. Grundsätzlich ist das hier bekanntgewordene Vorgehen der Hochschulen datenschutzrechtlich nicht zu beanstanden, da man sich in der Regel an Folgendes hält:

Im Prüfungsverfahren muss auf den Grundsatz der Chancengleichheit besonders geachtet werden. Wer im Verhältnis der Kandidaten untereinander einen rechtlichen Vorteil in dem Sinne für sich in Anspruch nehmen will, dass ein von ihm offiziell angemeldeter Prüfungstermin nicht zählen soll, obwohl er insoweit in einem Prüfungsrechtsverhältnis steht, das ihn zum Antritt zur Prüfung wie alle übrigen Kandidaten verpflichtet, hat die für die Nichtanrechnung des Prüfungstermins tragenden Gründe glaubwürdig und nachvollziehbar offenzulegen.

Im Falle des Rücktritts von der Prüfung oder des Versäumnisses hat der Prüfling hierfür triftige Gründe dem Prüfungsausschuss bzw. dem Prüfungsamt unverzüglich mitzuteilen und glaubhaft zu machen, so wie es die Prüfungsordnungen vorsehen. Dies kann insbesondere durch ein qualifiziertes Attest geschehen.
Prüfungsunfähigkeit liegt nur dann vor, wenn durch eine Beeinträchtigung des gesundheitlichen Wohlbefindens der Aussagewert einer Prüfungsleistung für die wirklichen Fähigkeiten und Kenntnisse des Prüflings erheblich eingeschränkt ist und die Prüfung damit ihren Zweck verliert, Aufschluss über die Befähigung für einen bestimmten Beruf oder für eine bestimmte Ausbildung zu geben. Diese Voraussetzungen treffen nur auf Krankheitsbilder mit aktueller und zeitweiliger Beeinträchtigung des physischen und/oder psychischen Wohlbefindens zu.

Ob Prüfungsfähigkeit vorliegt, ist zunächst eine medizinische, aber nicht ausschließlich medizinische Frage, die abschließend von der Prüfungsbehörde zu entscheiden ist. Damit die Prüfungsbehörde zu einer solchen Entscheidung überhaupt in der Lage ist, bedarf es aber bestimmter Angaben, die in dem ärztlichen Attest vorzusehen sind:

- Dauer der Erkrankung,
- Termine der ärztlichen Behandlung,
- Art und Umfang der Erkrankung unter Angabe der vom Arzt aufgrund eigener Wahrnehmung getroffenen Tatsachenfeststellungen,
- Auswirkungen der Erkrankung auf die Prüfung.

Das ärztliche Attest muss darüber hinaus in einer auch für den Laien nachvollziehbaren Sprache verfasst sein.

Nur Vertreter der Prüfungsbehörde und die Prüfer dürfen Einblick in die eingereichten ärztlichen Atteste nehmen. Sie müssen über deren Inhalt Stillschweigen bewahren.

8.3 Wissenschaft

8.3.1 Genetische Vaterschaftstests

Die Datenschutzbeauftragten des Bundes und der Länder hatten sich in ihrer Entschließung vom Herbst 2001 gegen heimliche Vaterschaftstests ausgesprochen. Die Entscheidungen des BGH (Urteile vom 12. Januar 2005 – XII ZR 60/03 und XII ZR 227/03), wonach Anfechtungsklagen nicht auf heimliche Vaterschaftstests gestützt werden dürfen, sowie erste Pläne des Gesetzgebers, solche Tests zu verbieten, haben die öffentliche Diskussion wieder angefacht. Das Meinungsbild ist sehr unterschiedlich: Einerseits wird gefordert, das Recht des Vaters auf Wissen um seine biologische Vaterschaft nicht zu beschneiden, andererseits soll der Persönlichkeitsschutz des Kindes nicht unnötig eingeschränkt werden.

Aufgrund der aktuellen Diskussion haben die Datenschutzbeauftragten sich erneut öffentlich geäußert: In einer gemeinsamen Presseerklärung (vgl. Anlage 16) fordern sie, Gentests ohne Wissen der Betroffenen zu untersagen.

Die heimlichen genetischen Vaterschaftstests werfen zahlreiche Fragen auf, zum Beispiel:

- Ist die Einwilligung der Mutter erforderlich, wenn das 16-jährige Kind wissen will, ob sein Vater auch sein Erzeuger ist?
- Wer muss einwilligen, wenn die Mutter einen Test fordert, weil sie z. B. glaubt, ihr Kind sei in der Geburtsklinik verwechselt worden?
- Wie ist die Situation bei Adoptiveltern?
- Wird die Familie nicht weniger belastet, wenn der Vater bei Zweifeln heimlich einen Test durchführt und das Ergebnis für sich behält?
- Wie wird sichergestellt, dass die vorliegenden Proben auch tatsächlich von Vater und Kind stammen?
- Wenn die Einwilligung der Mutter erforderlich ist, kann diese bei Verweigerung z. B. durch das Jugendamt ersetzt werden?
- Reichen die bisherigen Rechtsmittel der Vaterschaftsklage aus, um die Rechte des vermeintlichen Vaters zu schützen?
- Ist auch die Mutter Betroffene beim Gentest oder willigt sie nur in gesetzlicher Vertretung für ihr Kind ein?
- Kann die Mutter überhaupt unbefangen im Interesse ihres Kindes handeln?
- Wird überhaupt eine Mutter einwilligen, wenn sie durch einen Test Gefahr läuft, einen zahlenden Vater zu verlieren?

Die Beantwortung dieser und weiterer Fragen ist nicht nur Sache des Datenschutzes.

8.3.2 Onkologisches Nachsorgeprogramm

Menschen, die an Krebs erkrankt waren, aber inzwischen tumorfrei sind, können an einem Nachsorgeprogramm teilnehmen. In dessen Rahmen können sie sich durch die Kassenärztliche Vereinigung an Untersuchungstermine erinnern lassen und ihre Gesundheitsdaten für wissenschaftliche Zwecke zur Verfügung stellen. Die Dokumentation des Nachsorgeprogramms übernimmt das Tumorzentrum Rheinland-Pfalz. Die Patienten erhalten einen Nachsorgepass, aus dem sich genau ergibt, wer welche Daten im Nachsorgeprogramm erhält und verarbeitet. Die Patienten willigen in die Datenverarbeitungsvorgänge mit ihrer Unterschrift im Nachsorgepass ein, so dass diese auf einer wirksamen Einwilligung der Betroffenen gem. § 5 LDSG beruhen. Änderungen bzw. Ergänzungen der Einwilligungserklärung, die aus Sicht des Tumorzentrums notwendig sind, werden von dort frühzeitig mit dem LfD abgestimmt. So wurde im Berichtszeitraum ein Passus eingefügt, wonach Patientendaten an Kliniken, bei denen der Patient in Behandlung war und von denen er zur Nachsorge angemeldet wurde, übermittelt werden dürfen zu Zwecken der Qualitätssicherung und wissenschaftlichen Auswertung.

8.3.3 „Befehl ist Befehl“

Das ISM plante eine Ausstellung über die Polizei in der NS-Zeit. Dabei sollten auch Lebensläufe von Polizeibeamten veröffentlicht werden, die während dieser Zeit in Ausübung ihrer Tätigkeit strafbare Handlungen begangen und dennoch nach 1945 erneut Karriere im Polizeidienst gemacht hatten. Dies betraf den ehemaligen Leiter des Landeskriminalamtes und den ehemaligen Leiter der Kriminalpolizei Ludwigshafen. Die Informationen stammten teilweise aus den Personalakten der Betroffenen.

Die Verwendung der personenbezogenen Daten für die Ausstellung war nach den Vorschriften des Landesarchivgesetz zu beurteilen, da die Personalakten der Betroffenen zwischenzeitlich einem Archiv übermittelt worden waren. Nach § 3 Abs. 1 LArchG darf jeder, der ein berechtigtes Interesse darlegt, öffentliches Archivgut nach Maßgabe der Rechtsvorschriften und der Benutzungsordnung nutzen. Die Nutzung ist jedoch an bestimmte Fristen gebunden, soweit es sich um Daten natürlicher Personen handelt. Diese dürfen gem. § 3 Abs. 3 S. 2 LArchG grundsätzlich erst 30 Jahre nach dem Tod der Person genutzt werden. Diese Frist wurde hier eingehalten, da die Betroffenen bereits länger als 30 Jahre tot waren. Eine andere Frist gilt jedoch für Unterlagen aus den Personalakten der Polizeibeamten: Da diese aufgrund von Rechtsvorschriften geheim zu halten sind, dürfen sie gem. § 3 Abs. 3 S. 4 LArchG erst 80 Jahre nach ihrer Entstehung genutzt werden. Diese Frist war bei den zur Veröffentlichung bestimmten Unterlagen aus den Personalakten noch nicht abgelaufen. Sie kann jedoch gem. § 3 Abs. 4 S. 2 LArchG für Personen der Zeitgeschichte verkürzt werden, wenn die schutzwürdigen Belange der Betroffenen angemessen berücksichtigt werden. Bei den Betroffenen handelte es sich aus Sicht des LfD durchaus um Personen der Zeitgeschichte. Auch waren hier ihre schutzwürdigen Belange grundsätzlich angemessen berücksichtigt, da zur Veröffentlichung hauptsächlich von den Betroffenen unterzeichnete Formblätter mit damals üblichen Erklärungen bestimmt waren. Fraglich war, ob dies auch auf den Brief eines Betroffenen an den ehemaligen Staatsminister Wolters zutraf, da dieser einen wesentlich persönlicheren Inhalt hatte. Zwar war der Brief ursprünglich nicht zur Veröffentlichung bestimmt, doch gab er in erster Linie die Leistungen des Absenders wieder, die ein positives Licht auf dessen Arbeit werfen sollten. Der Betroffene wollte damit erreichen, dass ein gegen ihn anhängiges Disziplinarverfahren ausgesetzt wird. Dass dies eine gewisse öffentliche Wirkung erzielen könnte, war ihm sicherlich bewusst und auch nicht unbeabsichtigt. Daher waren auch bei der Nutzung dieses Schriftstückes die schutzwürdigen Belange des Betroffenen angemessen berücksichtigt.

Zudem wurden auch persönliche Daten von Polizeibeamten veröffentlicht, die während der NS-Zeit entgegen den damaligen Befehlen gehandelt hatten. Bei diesen wurde die Veröffentlichung zuvor mit den Angehörigen abgestimmt, so dass in diesem Fall keine schutzwürdigen Belange entgegenstanden.

9. Umweltschutz

9.1 Die Schaffung eines Landesumweltinformationsgesetzes

Das Umweltinformationsgesetz in der Fassung der Bekanntmachung vom 23. August 2001 wurde anlässlich europarechtlicher Vorgaben durch das Gesetz zur Neugestaltung des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I, S. 3740) aufgehoben. Im Gegensatz zur früheren Rechtslage hat der Bund keine bundesweit geltende Regelung zum Umweltinformationsrecht getroffen, sondern eigene Bestimmungen nur für die informationspflichtigen Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts erlassen, so dass diesbezüglich in Rheinland-Pfalz – wie in allen anderen Bundesländern – ein eigenes Landesgesetz geschaffen werden muss, das sich gegenwärtig in der parlamentarischen Beratung befindet.

Der Gesetzentwurf der Landesregierung zum Landesumweltinformationsgesetz (LT-Drs. 14/4307) bezweckt die Umsetzung der Aarhus-Konvention aus dem Jahre 1998, die aufgrund einer entsprechenden EG-Richtlinie (2003/4/EG) in deutsches Recht zu überführen ist. In der Aarhus-Konvention (vgl. dazu 17. Tb., Tz. 9.2) haben sich die Unterzeichnerstaaten, zu denen auch die Bundesrepublik Deutschland gehört, verpflichtet, ihren Bürgern und Organisationen mehr Rechte und Pflichten beim Schutz der Umwelt zu gewähren. Diesem Ziel dient ein verbesserter Zugang zu Informationen über die Umwelt.

Der LfD erhielt bereits frühzeitig Gelegenheit, sich zum Entwurf des Landesumweltinformationsgesetzes zu äußern. Er konnte den darin enthaltenen datenschutzbezogenen Aussagen im Wesentlichen zustimmen. So ist die Regelung in § 9 bzgl. des Schutzes privater Belange hinreichend klar, um zu gewährleisten, dass auch bei Ausübung des neuen Einsichtsrechts in Umweltakten das Grundrecht auf informationelle Selbstbestimmung grundsätzlich gewährleistet bleibt. Es ist eine Abwägung mit dem öffentlichen Interesse an der Bekanntgabe der Umweltdaten vorgesehen. Hier hatte der LfD im Rahmen seiner Stellungnahme zum Gesetzentwurf angeregt – zumindest im Begründungsteil – klarstellend darzulegen, welche datenschutzrechtlichen Vorgaben zur Anwendung kommen, wenn es um die in der Praxis oft schwierige Abwägung von Rechten des Einzelnen mit den Interessen der Allgemeinheit geht. Er hat darauf hingewiesen, dass bei der Abwägung insbesondere auch die datenschutzrechtlichen Vorgaben der Europäischen Gemeinschaft, vor allem deren Konkretisierung in der EG-Datenschutzrichtlinie zu berücksichtigen sind.

Der Gesetzgeber hat diese Anregung aufgegriffen. In der Begründung zum Entwurf des Landesumweltinformationsgesetzes zu § 9 heißt es nunmehr:

„Absatz 1 Satz 1 Nr. 1 dient dem Schutz des Grundrechts auf informationelle Selbstbestimmung, das nach Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 des Grundgesetzes als Bestandteil des allgemeinen Persönlichkeitsrechts geschützt wird. (…) Bei der Abwägung des öffentlichen Interesses auf Zugang zu Umweltinformationen mit dem Grundrecht auf informationelle Selbstbestimmung sind die Vorgaben der EG-Datenschutzrichtlinie (95/46/EG; Amtsblatt EG-L 281, S. 31) zu beachten, insbesondere die Art. 6, 7, 10–12 und 17. Diese Vorgaben sind im Landesdatenschutzgesetz umgesetzt; hier ist insbesondere auf die §§ 5, 6, 13 und 16 hinzuweisen."

Gegenüber der bisherigen Rechtslage aufgrund des früheren Bundes-Umweltinformationsgesetzes in der Fassung vom 23. August 2001 (BGBl. I S. 2218, vgl. hierzu 17. Tb., Tz. 9.1) werden folgende Änderungen eintreten:

- Das individuelle Zugangsrecht wird um eine Pflicht zur aktiven Umweltinformation ergänzt. Die Verwaltung muss Orientierungshilfen bei der Suche nach Umweltinformationen bieten. Zum Mindestinhalt der aktiv zu verbreitenden Daten gehören: Rechtsgrundlagen, Überwachungsergebnisse, Genehmigungen mit erheblichen Auswirkungen, Daten aus der Umweltverträglichkeitsprüfung und Risikobewertungen.
- Der Begriff der Umweltinformationen wird erweitert (menschliche Gesundheit, Gentechnik).
- Öffentliche und private Belange der Geheimhaltung müssen jetzt zusätzlich mit dem Zugangsinteresse abgewogen werden.
- Der Adressatenkreis umfasst nun auch Privatunternehmen, die öffentliche Verwaltungsaufgaben im Umweltbereich wahrnehmen und deren Unternehmensstrategie maßgeblich vom Land oder den Kommunen bestimmt werden kann (z. B. Stadtwerke GmbH, Verkehrsbetriebe).

9.2 Einführung des Anlageninformationssystems – Immissionsschutz (AIS-I) in der rheinland-pfälzischen Umweltverwaltung

AIS-I ist ein modulares Anlageninformationssystem für den Immissionsschutz, das die für den Vollzug des Bundesimmissionsschutzgesetzes zuständigen Behörden umfassend unterstützt. Der modulare Aufbau bietet die Möglichkeit, das System für zusätzliche Anforderungen, die sich aus neuen gesetzlichen Vorgaben ergeben, zu erweitern und differenzierte Schreib- und Leserechte für einzelne Module zu vergeben. Das Projekt AIS-I wurde 1994 von den Umweltministerien der Länder Sachsen und Brandenburg gemeinsam entwickelt. Zwischen 1997 und 2003 haben sich Mecklenburg-Vorpommern, Niedersachsen, Schleswig-Holstein, Thüringen und Hessen der Länderkooperation angeschlossen. In Rheinland-Pfalz wurde die neue Fachanwendung Anfang 2005 in Betrieb genommen. Die Programmentwicklung erfolgt entsprechend den Anforderungen der beteiligten Länder. Sie betreiben die Anwendung jeweils in eigener Verantwortung, eine Vernetzung bzw. ein Datenaustausch mit anderen „AIS-I-Ländern“ existiert nicht. AIS-I besteht aus neun Komponenten, wobei in Rheinland-Pfalz zunächst lediglich die Module A (Arbeitsstätten- und Anlagenverwaltung) und E (Emmissionserklärung) genutzt wurden. Nunmehr ist vorgesehen, auch die Module Ü (Überwachungstätigkeit) und N (Nachbarschaftsbeschwerden) zu integrieren. Soweit gegenwärtig ersichtlich, werden hierbei im Vollzug des Bundesimmissionsschutzgesetzes anfallende personenbezogene Daten von Widerspruchsführenden in Genehmigungsverfahren, von Einwendenden bei Öffentlichkeitsbeteiligung und von Beschwerdeführenden bei Nachbarschaftsbeschwerden gespeichert.

Der LfD wird das Verfahren datenschutzrechtlich begleiten mit dem Ziel, den Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen so gering wie möglich zu halten. Das für die Umsetzung zuständige Landesamt für Umweltschutz und Gewerbeaufsicht hat bereits angekündigt, eine datenschutzfreundliche Lösung zu entwickeln.

10. Gesundheitswesen

10.1 Elektronische Gesundheitskarte

Bei der zum 1. Januar 2006 gesetzlich vorgesehenen Einführung einer elektronischen Gesundheitskarte, die die bisherige Krankenversichertenkarte ablösen soll, handelt es sich um eines der ehrgeizigsten, aufwändigsten und technisch schwierigsten Vorhaben, an dessen Umsetzung gegenwärtig in der Bundesrepublik Deutschland gearbeitet wird. Auch wenn nicht zu erwarten ist, dass bis zum Stichtag sämtliche der in § 291 a SGB V enthaltenen Anwendungen realisiert werden können, ist doch die Entwicklung hin zur Einbindung der Telematik in das Gesundheitswesen nicht mehr aufzuhalten. Die Belange des Datenschutzes haben in der vorgenannten Regelung ihren Niederschlag gefunden. Dies ist ausdrücklich zu begrüßen.

10.1.1 Entwicklungen auf Bundesebene

Die im Zuge der Einführung der elektronischen Gesundheitskarte aus datenschutzrechtlicher Sicht zu beachtenden Gesichtspunkte haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung im Rahmen ihrer 69. Konferenz (vgl. Anlage 13) noch einmal benannt. In enger Abstimmung mit den Landesbeauftragten hat der BfD wiederholt im Vorfeld der geplanten Einführung – beispielsweise im Zusammenhang mit der Erstellung der zugrunde liegenden technischen Rahmen- und Lösungskonzepte – die Berücksichtigung dieser datenschutzrechtlichen Anliegen gefordert. Es bleibt abzuwarten, wie die inzwischen zur Schaffung einer für die Einführung und Anwendung der elektronischen Gesundheitskarte erforderlichen Telematikinfrastruktur gebildete Gesellschaft für Telematik diesen berechtigten Belangen des Datenschutzes entsprechen wird.

Angesichts der Freiwilligkeit der in § 291 a Abs. 3 SGB V enthaltenen Anwendungen kann nur eine datenschutzgerechte, sichere und das Patientengeheimnis wahrende Ausgestaltung der elektronischen Gesundheitskarte zum Erfolg führen und die damit erhofften Kosteneinsparungen und qualitativen Verbesserungen in der medizinischen Versorgung erreichen. Denn ohne die Akzeptanz der in erster Linie hiervon betroffenen Leistungserbringer und Patienten dürften die mit der Einführung von Telematikanwendungen im Gesundheitsbereich verbundenen Chancen wohl ungenutzt bleiben.

10.1.2 Das Modellprojekt „Elektronische Gesundheitskarte Rheinland-Pfalz“ in der Region Trier

Das von der Kassenärztlichen Vereinigung Trier (seit dem 1. Januar 2005: Kassenärztliche Vereinigung Rheinland-Pfalz) getragene Modellprojekt „Elektronische Gesundheitskarte Rheinland-Pfalz“ erprobt als bundesweit einziges derartiges Vorhaben unter Teilnahme von ca. 50 Arztpraxen, zwei Krankenhäusern und weiteren Institutionen in einer ersten Phase die Anwendung einer elektronischen Patientenakte. Dabei findet die elektronische Behandlungsdokumentation anonymisiert und verschlüsselt auf einem zentralen Server statt, während die eingesetzte Karte als Zugangsschlüssel dient und selbst keine medizinischen Daten speichert. Das Vorhaben nahm am 29. November 2004 seinen Echtbetrieb auf und ist zunächst bis zum 31. Dezember 2006 befristet.

Im Ergebnis hatte der LfD, der von Beginn an von den am Projekt beteiligten Institutionen eingebunden wurde, auf der Grundlage der ihm zur Verfügung gestellten Informationen keine grundsätzlichen datenschutzrechtlichen Bedenken gegen das Vorhaben geäußert. Die Projektverantwortlichen wurden allerdings in verschiedenen Zusammenhängen um Nachbesserungen oder Ergänzungen gebeten.

– Einverständnis- und Teilnahmeerklärung/Patienteninformation:

  An der Textgestaltung der Einverständnis- und Teilnahmeerklärung sowie der Patienteninformation war der LfD maßgeblich beteiligt. Insbesondere erfolgte auf seine Anregung eine Differenzierung zwischen Informations- und Erklärungstext.

– Kryptografie:

  Das Vorhaben nutzt für die Verschlüsselung der Behandlungs- und Verzeichniseinträge sowie die Transportverschlüsselung bei der Übertragung von Daten zum Index- und Datenserver unterschiedliche symmetrische Verfahren. Für die Authentisierung bei Speicherung und Abruf von Behandlungseinträgen kommen asymmetrische Verfahren zum Einsatz. Bei den genutzten Algorithmen und Schlüssellängen handelt es sich um gängige Lösungen, die aus Sicht des LfD keinen Bedenken begegnen. Die kryptografischen Parameter sind derzeit fest vorgegeben. Um einer im Zeitverlauf gegebenenfalls erforderlichen Anpassung von Algorithmen oder Schlüssellängen an veränderte Rahmenbedingungen rasch entsprechen zu können, hat der LfD empfohlen, in den Verzeichniseinträgen Angaben vorzusehen, die eine Nutzung unterschiedlicher Kryptoverfahren erlauben.

– Zugriffsrechte:

  Angesichts der Speicherung von Behandlungseinträgen unterschiedlicher Leistungserbringer und der in § 291 a Abs. 5 Satz 2 SGB V vorgesehenen Autorisierung der Versicherten sollten Zugriffsrechte differenziert vergeben werden können. Dem wurde mit der zusätzlichen Speicherung von Freigabeinformationen zu jedem Akteneintrag, die die Vergabe individueller Zugriffsbefugnisse für einzelne Leistungserbringer ermöglichen, entsprochen. Im Rahmen des Modellversuchs ist dies jedoch zunächst auf Berufs- oder Facharztgruppen beschränkt.

– Wahrnehmung von Patientenrechten:

  Zur Wahrung der Betroffenenrechte hatte der LfD empfohlen, Funktionen vorzusehen, die den Patienten gegebenenfalls eigenständig eine verständliche Anzeige und den Ausdruck der Inhalte der Gesundheitsakte gestatten. Dies wurde mit der Schaffung von Anzeige- und Druckmöglichkeiten umgesetzt. Bislang können diese jedoch nur in der Praxis des betreuenden Arztes genutzt werden. Es ist vorgesehen, derartige Zugriffsmöglichkeiten der Patienten auch außerhalb der Arztpraxen einzurichten.

– Protokollierung:

  Das Verfahren sieht gegenwärtig eine Protokollierung von Zugriffen sowohl auf der Karte als auch beim Server vor. Die Angaben auf der Karte lassen für die letzten 50 Zugriffe allerdings lediglich erkennen, durch welche Stelle auf Verwaltungs-, Notfall- oder Aktendaten allgemein ein lesender bzw. schreibender Zugriff erfolgt ist. Der Patient kann so nachvollziehen, bei welcher Gelegenheit die Karte genutzt wurde. Welcher Behandlungseintrag wann durch welche Stelle neu angelegt, geändert oder ausgelesen wurde, ergibt sich daraus jedoch nicht.

  Im Hinblick auf die in § 291 a Abs. 6 SGB V enthaltenen Vorgaben sind Zugriffe auf Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte und Impfungen für Zwecke der Datenschutzkontrolle zu protokollieren. Nach Auffassung des LfD sind hierzu bezogen auf jeden Eintrag die zugreifende Stelle, Datum und Uhrzeit des Zugriffs, Art des Zugriffs (Lesezugriff, Änderung, Neuanlage, Löschung) und ggf. zusätzliche Angaben zu den beteiligten IT-Systemen zu erfassen. Die serverseitig vorgesehene Protokollierung beim Server berücksichtigt dies. Mit Blick auf die bestehende Pseudonymität der Verzeichnis- und Behandlungseinträge sollte es aber vermieden werden, Angaben in die Protokollierung aufzunehmen, anhand derer eine Zuordnung von Behandlungseinträgen zu Patienten möglich wäre (Nummer der Patientenkarte oder Teilnehmernummer des Patienten).

– Verfahren im Fall des Verlusts oder der Beschädigung der Karte:

  Von der Speicherung der Patientenstammdaten abgesehen dient die Chipkarte vorrangig dazu, den Datenzugriff zu steuern. Die für die individuelle Zuordnung von Behandlungseinträgen und deren Entschlüsselung benötigten Informationen werden ausschließlich auf der Karte gespeichert und liegen damit grundsätzlich in der alleinigen Verfügungsgewalt der Patienten. Dieses Prinzip wird insoweit durchbrochen, als für den Fall des Verlusts oder einer Beschädigung der Karte beim betreuenden Arzt eine Sicherheitskopie der Kartendaten einschließlich der für die Entschlüsselung der Behandlungseinträge erforderlichen Angaben vorgehalten wird.

Um eine kontrollierte Inanspruchnahme der Kartenkopie sicherzustellen, empfahl der LfD im Falle eines Zugriffs neben der Protokollierung eine verschlüsselte Speicherung der Kopie und das Vier-Augen-Prinzip. Die Anregungen des LfD wurden weitgehend aufgegriffen: für die Personalisierung von Ersatzkarten ist die Beteiligung eines Trustcenters sowie des Patienten verfahrensmäßig zwingend vorgesehen. Ohne den Patienten ist eine Nutzung der Kartenkopie nur bei missbräuchlichem Zusammenwirken von Arzt und Trustcenter denkbar. Im Rahmen des Modellversuchs begegnet dieses Verfahren zur Wiederherstellung der Kartendaten grundsätzlich keinen datenschutzrechtlichen Bedenken. Für eine Optimierung sollte jedoch die Verschlüsselung der Kartenkopie mit einem vom betreuenden Arzt unabhängigen Schlüssel geprüft werden, z. B. dem öffentlichen Schlüssel des Trustcenters.

Der LfD wird auch weiterhin die mit der Einführung der elektronischen Gesundheitskarte in Zusammenhang stehenden Entwicklungen kritisch beobachten und sich für eine datenschutzgerechte Ausgestaltung des Vorhabens einsetzen.

10.2 Verarbeitung von Gesundheitsdaten im Rahmen amtsärztlicher Untersuchungen

10.2.1 Datenverarbeitung bei der zentralen medizinischen Untersuchungsstelle

Mit der am 27. Oktober 2004 in Kraft getretenen Änderung des § 61 a LBG und der damit verbundenen Einrichtung einer zentralen medizinischen Untersuchungsstelle beim Landesamt für Soziales, Jugend und Versorgung soll ausweislich der Gesetzesbegründung das Verfahren zur Begutachtung der Dienstunfähigkeit unmittelbarer Landesbeamter beschleunigt und qualitativ verbessert werden. Nach der bisherigen Rechtslage untersuchte zunächst der Amtsarzt oder ein als Gutachter beauftragter Arzt den Betroffenen. In einem zweiten Schritt nahm dann die ehemalige zentrale medizinische Verbindungsstelle eigenständig Plausibilitätsprüfungen zur Qualitätssicherung vor und überprüfte die Einhaltung einheitlicher Bewertungsmaßstäbe. Die mit der Gesetzesänderung erfolgte Straffung und Zentralisierung des Verfahrens ist aus datenschutzrechtlicher Sicht zu begrüßen.

Im Berichtszeitraum war der LfD häufig mit Fragen des Datenschutzes im Zusammenhang mit der Durchführung von Verfahren zur Überprüfung der Dienstunfähigkeit unmittelbarer Landesbeamter befasst. Neben etlichen Eingaben zur Zulässigkeit der Weitergabe hierbei erhobener medizinischer Informationen (vgl. hierzu Tz. 10.2.2) stellte auch die Datenverarbeitung bei der zentralen medizinischen Untersuchungsstelle ein wichtiges Tätigkeitsfeld dar. Konkret war der LfD bei der Neugestaltung der von der Behörde einzusetzenden Vordrucke und Formulare eingebunden. Hierbei konnten unter datenschutzrechtlichen Gesichtspunkten deutliche Verbesserungen und Klarstellungen erreicht werden:

So sah der Vordruck für die Erteilung des Begutachtungsauftrages ursprünglich vor, dass die personalführenden Stellen u. a. auch allgemeine Erkenntnisse über den zeitlichen Umfang außerdienstlicher Engagements bzw. außerdienstlicher Belastungen der Betroffenen der zentralen medizinischen Untersuchungsstelle mitteilen sollten. Der Vordruck ließ offen, ob damit auch solche Informationen gemeint waren, die der personalführenden Stelle nicht aus dienstlichen Gründen bekannt wurden (z. B. durch privates Gespräch) bzw. die sonstige außerdienstliche Belastungen der Betroffenen wie z. B. Eheprobleme oder gesundheitliche Beeinträchtigungen naher Angehöriger betrafen. Es wurde vereinbart, die von der personalführenden Stelle erbetenen Angaben hinsichtlich außerdienstlicher Engagements bzw. Belastungen lediglich auf die sich aus der Personalakte ergebenden Erkenntnisse zu beschränken. Ansonsten hätten es die Betroffenen hinnehmen müssen, dass der zentralen medizinischen Untersuchungsstelle bloße Gerüchte mitgeteilt und der Untersuchung zugrunde gelegt werden. Die Möglichkeit, im Rahmen des Untersuchungsgesprächs derartige Informationen falls erforderlich von den Untersuchten direkt zu erheben, bleibt unbenommen.

Weiterhin enthält auf Anregung des LfD der in diesem Zusammenhang eingesetzte Anamnesebogen künftig nicht mehr die Frage nach einer bestehenden Schwangerschaft. Den Betroffenen wird zudem in dem an sie gerichteten Anschreiben die Beantwortung der auf dem Anamnesebogen erbetenen Angaben zur Familienvorgeschichte und zu eigenen Vorerkrankungen freigestellt. Denn angesichts der in diesem Zusammenhang bestehenden datenschutzrechtlichen Bedenken bezüglich der Verwendung von Fragebögen (vgl. 15. Tb., Tz. 10.2.2) sollte für den Betroffenen zumindest die Möglichkeit bestehen, in dem Untersuchungsgespräch mit dem Amtsarzt die sachliche Erforderlichkeit der erfragten Angaben selbst zu klären.

Im Hinblick auf die von den Betroffenen im Rahmen der Untersuchung abzugebenden Einverständniserklärung bzw. der darin enthaltenen Befreiung von der ärztlichen Schweigepflicht war zunächst fraglich, ob gegen den Verzicht der namentlichen Bezeichnung der Personen, die befreit werden sollen, datenschutzrechtliche Bedenken bestehen. Angesichts des sich jedoch regelmäßig bereits aus der Untersuchung ergebenden Personenkreises, den der Betroffene zudem ausdrücklich benennen muss, sowie der ebenfalls zu berücksichtigenden Anforderungen an ein schnelles und möglichst flexibles Beurteilungsverfahren ist es aus der Sicht des LfD noch hinnehmbar, wenn sich der Erklärungstext lediglich auf die von dem Untersuchten „genannten Personen oder Stellen“ bezieht, ohne deren Namen ausdrücklich zu nennen.

Der LfD wird auch in Zukunft die Tätigkeit der zentralen medizinischen Untersuchungsstelle beobachten.

10.2.2 Weitergabe medizinischer Informationen im Zusammenhang mit einer amtsärztlichen Untersuchung

Im Berichtszeitraum hatte sich der LfD wiederholt mit der Frage zu befassen, ob bzw. in welchem Umfang medizinische Informationen über Beschäftigte, die im Rahmen amtsärztlicher Untersuchungen gewonnen wurden, durch das Gesundheitsamt bzw. die auftraggebende Dienststelle weitergegeben werden dürfen.

In einem Fall hatte ein Gesundheitsamt auf Veranlassung des Polizeipräsidiums als personalaktenführender Stelle einen Polizeibeamten auf dessen Polizeidienstfähigkeit zu untersuchen. Nach erfolgter Untersuchung übermittelte das Gesundheitsamt dem auftraggebenden Polizeipräsidium neben dem Untersuchungsergebnis auch den genauen Untersuchungsbefund sowie detaillierte Angaben zum Krankheitsbild des Beamten. Dessen Dienstfähigkeit war danach aufgrund einer festgestellten behandlungsbedürftigen Bluthochdruckerkrankung sowie einer akuten depressiven Episode eingeschränkt. Das Polizeipräsidium befreite daraufhin den Betreffenden vorläufig von der Erbringung des Nachtdienstes. Zuvor hatte es den Dienststellenleiter der Polizeiinspektion, bei der der Beamte eingesetzt gewesen war, über die beabsichtigte Entscheidung und die zugrunde liegenden medizinischen Informationen unterrichtet.

Nach der in diesem Zusammenhang heranzuziehenden Regelung des § 61 a LBG teilt der Arzt nur im Einzelfall der Behörde das die tragenden Feststellungen und Gründe enthaltende Gutachten mit, soweit dessen Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist. Bezogen auf den dargestellten Sachverhalt führte dies zu folgendem Ergebnis:

Zunächst war hinsichtlich der von dem Gesundheitsamt an das Polizeipräsidium übermittelten medizinischen Informationen zu differenzieren.

- In Bezug auf die Blutdruckerkrankung hätte es ausgereicht, wenn statt der genauen Diagnose das Gesundheitsamt lediglich die sich hieraus für die weitere Dienstgestaltung ergebenden Folgerungen mitgeteilt hätte. Die Datenweitergabe war daher mangels Erforderlichkeit i. S. v. § 61 a LBG unzulässig. Daran änderte auch der Umstand nichts, dass im konkreten Fall der betroffene Polizeibeamte das Gesundheitsamt in Bezug auf eine Unterrichtung des Polizeipräsidiums von der ärztlichen Schweigepflicht befreit hatte. Denn der Gesetzgeber hat in § 61 a LBG eine abschließende Regelung getroffen, die selbst für eine mögliche sich auf die Datenweitergabe beziehende Einwilligungserklärung des Betroffenen keinen Raum mehr lässt. Maßgeblich für die Übermittlung der Gesundheitsdaten des Untersuchten an die Behörde sind nach § 61 a LBG ausschließlich der Verhältnismäßigkeits- und der Erforderlichkeitsgrundsatz.

- Anders musste dagegen die Unterrichtung des Polizeipräsidiums über die festgestellte psychische Erkrankung des Petenten bewertet werden. Angesichts der mit der Verrichtung des Polizeidienstes verbundenen Besonderheiten (Führen einer Dienstwaffe, hohe psychische Belastungen im Rahmen eines Diensteinsatzes) und den daraus resultierenden Fürsorgeaspekten des Dienstherrn war diese Information für die Frage weiterer Einsatzmöglichkeiten des Betroffenen von großer Bedeutung und folglich für die von dem Polizeipräsidium zu treffenden Entscheidungen auch erforderlich i. S. v. § 61 a LBG, so dass hiergegen keine datenschutzrechtlichen Bedenken bestanden.

Soweit darüber hinaus die den Polizeibeamten betreffenden medizinischen Informationen von dem Polizeipräsidium an die personalführende Stelle weitergegeben wurden, gilt das zur Datenübermittlung durch das Gesundheitsamt Festgestellte entsprechend. Während die Weitergabe der durch den Amtsarzt festgestellten Diagnose einer Blutdruckerkrankung an die Polizeiinspektion mangels Erforderlichkeit nicht von § 61 a LBG gedeckt war, bestanden gegen die Unterrichtung über eine bestehende psychische Erkrankung aus den o. g. Gründen keine Bedenken.

Weiterhin ist zu betonen, dass eine generelle, einzelfallunabhängige Befugnis zur Übermittlung dieser Daten von der personalverwaltenden Stelle an die einzelnen Dienstbehörden, bei denen der Betroffene eingesetzt wird, nicht den gesetzlichen Vorgaben entspricht. Insbesondere rechtfertigen weder Gesichtspunkte der Plausibilitätskontrolle des amtsärztlichen Gutachtens noch die Grundsätze des Berufsbeamtentums eine solche Generalisierung.

Nachdem sowohl das betroffene Gesundheitsamt als auch das Innenministerium und Polizeipräsidium die Rechtsauffassung des LfD teilten und diese künftig beachten werden, wurde von einer Beanstandung der festgestellten Datenschutzverstöße abgesehen.

10.3 Zugriffsberechtigungen auf Daten des Gesundheitsamtes

Von den Belangen des Datenschutzes völlig unbeeindruckt zeigte sich eine Kreisverwaltung, bei der zum zweiten Mal nach fünf Jahren örtliche Feststellungen im Gesundheitsamt getroffen wurden. Dabei stellte sich u. a. heraus, dass trotz der damaligen förmlichen Beanstandung durch den LfD noch immer sowohl der Landrat als auch der für das Gesundheitsamt zuständige Dezernent permanent auf sämtliche in Textverarbeitungsverfahren auf dem Server der Kreisverwaltung gespeicherte Dokumente des Gesundheitsamtes zugreifen konnten. Eine Protokollierung solcher Zugriffe war nicht vorgesehen. Daneben wurde die direkt an das Gesundheitsamt gerichtete Post unverändert zumindest stichprobenweise durch Stellen außerhalb des Gesundheitsamtes geöffnet und inhaltlich von dem Dezernenten überprüft, selbst wenn diese Schreiben eindeutig medizinische Inhalte betrafen. Weiterhin verfügte die Systembetreuung auf Datei- und Verzeichnisebene über uneingeschränkte Zugriffsrechte u. a. auch für Daten aus dem Bereich des Gesundheitsamtes. Es handelte sich hierbei neben dem Schriftverkehr insbesondere auch um Vermerke, die von den Ärzten im Rahmen der regelmäßigen Sprechstunden angefertigt waren. Bereits die Bezeichnung der Dokumente ließ die Betroffenen erkennen und zum Teil Rückschlüsse auf den Inhalt zu.

Die eingeräumten Zugriffsberechtigungen stellten sowohl eine Verletzung der ärztlichen Schweigepflicht, der auch die Amtsärzte des Gesundheitsamtes unterliegen, als auch der in § 11 Abs. 6 Satz 2 ÖGdG enthaltenen Regelung dar. Hiernach ist die innerbehördliche Organisation so zu gestalten, dass Geheimhaltungspflichten und insbesondere die ärztliche Schweigepflicht gewahrt werden können. Das ÖGdG lässt in § 11 Abs. 3 Satz 2 die Weitergabe personenbezogener Daten innerhalb der Behörde des öffentlichen Gesundheitsdienstes nur unter engen Voraussetzungen und damit abhängig von den Umständen des Einzelfalles zu. Eine generelle und undifferenziert eingerichtete Zugriffsberechtigung zugunsten des Landrates bzw. des Dezernenten auf sämtliche Dokumente des Gesundheitsamtes ist angesichts dieser klaren gesetzlichen Regelung auch nicht mit dem Hinweis auf deren Vorgesetztenfunktion zu rechtfertigen. Dabei ist zu berücksichtigen, dass in der Regel die Aufgaben eines Dienstvorgesetzten auch ohne Kenntnis von Daten, die durch das Arztgeheimnis geschützt sind – beispielsweise durch anonymisierte Daten – wahrgenommen werden können. Sollte es im Einzelfall dennoch erforderlich sein, personenbezogene medizinische Daten Dritter zu diesem Zweck zur Kenntnis zu nehmen, kann dies auf der Grundlage des § 11 Abs. 3, Abs. 2 Nr. 1 ÖGdG ausnahmsweise zulässig sein. In diesem Fall sollte allerdings die Erforderlichkeit der Kenntnisnahme der von der ärztlichen Schweigepflicht umfassten Angaben ausdrücklich festgestellt und dokumentiert werden.

Hinsichtlich der Zugriffsberechtigungen der Systemverwaltung bestehen aus Sicht des LfD keine Bedenken gegenüber einer Unterstützung der Anwender und der technischen Betreuung der eingesetzten Geräte durch Bedienstete der Kreisverwaltung, soweit dies unter Kontrolle des Gesundheitsamtes erfolgt. Auch eine Eingliederung der Rechner des Gesundheitsamtes in ein internes Netzwerk zum Zweck der Teilnahme an der behördeninternen elektronischen Kommunikation (z. B. E-Mail) oder für die gemeinsame Nutzung von Terminkalendern, Telefon- und Adressverzeichnissen o. ä. ist grundsätzlich unproblematisch, wenn auf den beteiligten Systemen keine dem Arztgeheimnis unterfallenden Daten gespeichert sind. Soweit allerdings derartige Daten betroffen sind, müssen geeignete Sicherungsmaßnahmen ergriffen werden. Dies betrifft sowohl die in Datenbanken gespeicherten Daten als auch solche in Textverarbeitungsdokumenten wie z. B. ärztliche Gutachten. Angesichts der sich aus dem technischen Betrieb der Systeme ergebenden Erfordernisse kann zwar grundsätzlich ein Lese- und Schreibzugriff auf die Dateien des Gesundheitsamtes erforderlich sein. Die Notwendigkeit, dabei auf die Dateiinhalte zuzugreifen, besteht jedoch grundsätzlich nicht. Die der ärztlichen Schweigepflicht unterliegenden Daten müssen vielmehr nach § 11 Abs. 3 Satz 2 und Abs. 6 ÖGdG einem Zugriff des nichtärztlichen Personals außerhalb der Kontrolle des Gesundheitsamtes entzogen sein. Soweit die Daten auf Systemen gespeichert werden, die im administrativen Zugriff der Systembetreuung der Kreisverwaltung stehen, müssen diese deshalb durch kryptografische Maßnahmen wie z. B. einer Datei- oder Verzeichnisverschlüsselung vor einer unzulässigen Preisgabe gesichert werden.

Insgesamt stellte die sich darbietende Situation einen erheblichen Verstoß gegen den besonderen Schutz der Gesundheitsdaten dar, der auch strafrechtliche Relevanz haben kann (vgl. § 203 Abs. 1 StGB). Aus der Sicht des LfD war die vorgefundene Lage gerade angesichts der bereits fünf Jahre zuvor erfolgten datenschutzrechtlichen Bewertung, die wegen der Schwere des Datenschutzverstoßes schon damals zu einer förmlichen Beanstandung führte, nicht länger hinzunehmen. Die Kreisverwaltung wurde deshalb zur unverzüglichen Beachtung der datenschutzrechtlichen Vorgaben aufgefordert. Dem wurde letztendlich auch entsprochen.

10.4 Gesundheitsberichterstattung

Ob die Gesundheitsämter personenbezogene Daten und insbesondere medizinische Informationen nur zum Zwecke der Gesundheitsberichterstattung erheben dürfen, hatte der LfD im Berichtszeitraum mehrfach zu klären.

Zunächst tauchte die Frage im Zusammenhang mit der von dem Landesamt für Soziales, Jugend und Versorgung betriebenen Neufassung der Elternfragebögen auf, die bei den Einschulungsuntersuchungen eingesetzt werden. Dabei war geplant, zum Zwecke der Schaffung eines geeigneten Instrumentariums für die Planung von Präventionsmaßnahmen und zur Steuerung gesundheitspolitischer Entscheidungen künftig auch solche Informationen von den Betroffenen zu erheben, die selbst nicht unmittelbar den Zwecken der Schuleingangsuntersuchung dienen, die aber für die übergeordneten Aspekte der Gesundheitsberichterstattung nützlich wären.

In einem anderen Fall bat ein Krankenhaus den LfD um datenschutzrechtliche Prüfung einer Anfrage des örtlich zuständigen Gesundheitsamtes. Dieses hatte das Krankenhaus gebeten, zur Erarbeitung eines regionalen Gesundheitsberichtes verschiedene Patientendaten (Patientennummer, Alter, Geschlecht, Beruf, Postleitzahl des Wohnortes, Einweisungs-, Aufnahme- und Entlassungsdiagnose, Einweisungs- und Entlassungsdatum, Krankenkasse) dem Gesundheitsamt zu übermitteln. Angesichts der Personenbeziehbarkeit der Daten hatte das Krankenhaus Zweifel an der Zulässigkeit des Übermittlungsgesuchs.

Nach § 10 Abs. 2 Satz 1 ÖGdG stellen grundsätzlich die Behörden des öffentlichen Gesundheitsdienstes auf der Grundlage der bei ihnen vorhandenen gesundheitsbezogenen Daten die für die Erstellung des Gesundheitsberichts erforderlichen Daten in anonymisierter Form zusammen und übermitteln diese in aggregierter Form an das fachlich zuständige Ministerium. Das Gesetz geht somit von der Vorstellung aus, dass die Gesundheitsbehörden ausschließlich die ohnehin bei ihnen bereits vorhandenen Gesundheitsdaten für die Zwecke der Gesundheitsberichterstattung verarbeiten. Abgesehen von den erst durch ministerielle Anordnung in Betracht kommenden statistischen Erhebungen nach § 10 Abs. 2 Satz 2 ÖGdG hat der Gesetzgeber den Behörden des öffentlichen Gesundheitsdienstes auch keine eigene auf einer rechtlichen Regelung basierende ausdrückliche Datenerhebungsbefugnis zum Zwecke der Gesundheitsberichterstattung zuerkannt.

In Anbetracht der dem Allgemeinwohl dienenden Ziele einer umfassenden und validen Gesundheitsberichterstattung sowie unter Berücksichtigung der in § 11 Abs. 1 ÖGdG enthaltenen Regelung kann gleichwohl eine Erhebung personenbezogener Daten durch die Behörden des öffentlichen Gesundheitsdienstes, sofern dies ausschließlich zum Zwecke der Erstellung von Gesundheitsberichten erfolgt, auf der Basis einer informierten Einwilligung gem. § 5 Abs. 2 LDSG zulässig sein. Dabei sollten die hiervon Betroffenen neben der Freiwilligkeit zumindest über den Zweck der Verarbeitung, den möglichen Empfängerkreis der erhobenen Angaben sowie die Dauer der personenbezogenen Speicherung der Daten aufgeklärt werden.

Im Hinblick auf die Datenerhebung im Zusammenhang mit der Schuleingangsuntersuchung wies der LfD darauf hin, dass angesichts der unterschiedlichen rechtlichen Grundlagen der Datenverarbeitungen einerseits zum Zwecke der Feststellung der Schulreife, andererseits zur Erstellung von Gesundheitsberichten, eine deutliche Trennung dieser beiden Komplexe erfolgen muss. Denn während die Schuleingangsuntersuchung für die Betroffenen verpflichtend ist und von diesen nicht verweigert werden kann, obliegt es deren Entscheidung, ob sie darüber hinaus weitere Angaben machen, die nicht der Feststellung der Schultauglichkeit des Kindes dienen.

Das LSJV passte die in diesem Zusammenhang eingesetzten Unterlagen den datenschutzrechtlichen Vorgaben an.

10.5 Datenschutz bei der Suchtberatung

Im Rahmen einer Eingabe hatte der LfD folgenden Sachverhalt zu bewerten:

Nachdem aufgrund eines allgemeinen Informationsgesprächs bei der Beratungsstelle des Sozialpsychiatrischen Dienstes einer Kreisverwaltung bekannt wurde, dass möglicherweise ein in einem sicherheitsrelevanten Bereich Tätiger alkoholkrank ist, schaltete die Behördenmitarbeiterin zur Klärung der weiteren Vorgehensweise die Leitung des Sozialpsychiatrischen Dienstes ein. Diese führte mit dem Betroffenen ein weiteres Beratungsgespräch, in dem dieser sich zwar nicht als alkoholabhängig bezeichnete, allerdings ein Alkoholproblem selbst einräumte. Die von dem Amtsarzt angesichts der beruflichen Verwendung des Petenten angeregte Blutuntersuchung lehnte dieser ab. Daraufhin sprach das Gesundheitsamt eine sog. „Behandlungsauflage nach dem PsychKG“ aus, nach der sich der Betroffene zu einer weiteren Untersuchung im Gesundheitsamt einfinden sollte. Den vorgeschlagenen Termin sagte der Petent ab. Zugleich teilte er dem Gesundheitsamt mit, dass er selbst mit dem ärztlichen Dienst seines Arbeitgebers einen Gesprächstermin vereinbart habe. Der Amtsarzt informierte seinen Dienstvorgesetzten sowie die Rechtsabteilung der Kreisverwaltung hiervon und stimmte mit diesen die weiteren Schritte ab. Angesichts des angekündigten Gesprächs des Betroffenen mit dem ärztlichen Dienst des Arbeitgebers wurde die Behandlungsauflage als erfüllt angesehen; der Amtsarzt bat zugleich jedoch um eine zeitnahe schriftliche Bestätigung der angekündigten Untersuchung. Dem kam der Petent nicht nach. Das Gesundheitsamt sprach darauf hin erneut eine Behandlungsauflage aus, der der Betroffene entweder durch eine Untersuchung im Gesundheitsamt oder durch einen niedergelassenen Arzt oder durch Einschaltung des ärztlichen Dienstes seines Arbeitgebers nachkommen könne. Für den Fall der Nichtbefolgung stellte das Gesundheitsamt die Unterrichtung des ärztlichen Dienstes des Arbeitgebers in Aussicht.

Der Petent hielt sowohl die verwaltungsinterne Weitergabe der in einem vertraulichen Beratungsgespräch von ihm freiwillig mitgeteilten Informationen als auch die angedrohte Unterrichtung seines Arbeitgebers für datenschutzrechtlich unzulässig. Die Bewertung der Angelegenheit durch den LfD kam dagegen zu einem anderen Ergebnis:

Soweit die Mitarbeiterin der Beratungsstelle die im ersten Gespräch erhaltenen Informationen an die Leitung des Sozialpsychiatrischen Dienstes weitergegeben hatte, war dies von der Regelung des § 34 Abs. 5, Abs. 3 Satz 1 Nr. 1 a, c PsychKG gedeckt. Denn aufgrund dieser Angaben war zu befürchten, dass der Petent an einer Alkoholerkrankung leidet und dies darüber hinaus aufgrund seiner beruflichen Tätigkeit in einem sicherheitsrelevanten Bereich eine Gefährdung nicht nur seiner Gesundheit, sondern auch der mittelbar davon Betroffenen darstellt. Angesichts dieser Situation war zu entscheiden, ob aufgrund der in dem Beratungsgespräch mitgeteilten Informationen ein Tätigwerden des Gesundheitsamtes auf der Grundlage des § 8 PsychKG bzw. eine sofortige Unterrichtung des ärztlichen Dienstes des Arbeitgebers zur Abwendung der o. g. Gefährdung auf der Grundlage des § 34 Abs. 5 PsychKG erfolgen musste. Angesichts der Komplexität und Tragweite der zu treffenden Entscheidung war es gerechtfertigt, dass die Leitung des Sozialpsychiatrischen Dienstes selbst dies entschied, so dass eine Weitergabe der zugrunde liegenden Informationen an sie erforderlich war, zumal angesichts der betroffenen Rechtsgüter das Geheimhaltungsinteresse des Petenten deutlich zurücktrat.

Auch die im weiteren Verlaufe erfolgte Einbindung des Landrates und des Rechtsreferates der Kreisverwaltung durch den Amtsarzt bzw. die damit verbundene Weitergabe der den Petenten betreffenden Angaben war auf der Grundlage des § 34 Abs. 5, Abs. 3 Satz 1 Nr. 1 a, c PsychKG datenschutzrechtlich zulässig. Nach der Weigerung des Petenten zur Kooperation mit dem Gesundheitsamt musste auch hier – ähnlich der Situation unmittelbar nach dem ersten Beratungsgespräch – über das weitere Vorgehen entschieden werden. Da der Petent bislang eine Klärung der Frage, ob er tatsächlich alkoholkrank sei, verweigerte, stellte sich die Frage, ob und in welcher Weise das Gesundheitsamt nun tätig werden musste. Auch hier war aufgrund der Komplexität und Tragweite der zu treffenden Entscheidung eine Hinzuziehung des Landrates als Dienstvorgesetzten bzw. des Rechtsreferates zur Klärung des rechtlichen Hintergrundes gerechtfertigt und erforderlich.

Schließlich bestanden aus datenschutzrechtlicher Sicht auch keine Bedenken gegen die von dem Gesundheitsamt für den Fall der Nichtbefolgung der Behandlungsauflage angekündigte Unterrichtung des ärztlichen Dienstes des Arbeitgebers. In diesem Zusammenhang war insbesondere zu berücksichtigen, dass das Gesundheitsamt dem Petenten mehrere Möglichkeiten offen ließ, in

welcher Weise der Behandlungsauflage entsprochen werden konnte und somit nicht zwingend eine Unterrichtung des ärztlichen Dienstes des Arbeitgebers verlangt wurde. Angesichts der aus Sicht des Gesundheitsamtes gegebenen Gefahrenlage musste jedoch definitiv geklärt werden, ob der Petent tatsächlich alkoholkrank war. Hierzu durfte das Gesundheitsamt – zumindest bei nicht vorliegender Kooperationsbereitschaft des Petenten – auf der Grundlage des § 34 Abs. 5, Abs. 3 Satz 1 Nr. 1 a, c PsychKG den ärztlichen Dienst des Arbeitgebers unterrichten.

10.6 Outsourcing im Krankenhaus

10.6.1 Bestellung eines externen Datenschutzbeauftragten

Aufgrund der Anfrage eines „frei schaffenden Datenschützers“ hatte der LfD zu der Frage Stellung zu nehmen, ob der Kenntnisnahme von Patientendaten durch einen externen Krankenhausdatenschutzbeauftragten datenschutzrechtliche Gründe entgegenstehen.

Nach § 36 Abs. 8 Satz 2 LKG hat der Krankenhausträger nach den für ihn geltenden datenschutzrechtlichen Bestimmungen einen Beauftragten für den Datenschutz zu bestellen. Das für öffentliche Stellen maßgebliche LDSG sieht in § 11 Abs. 1 Satz 5 vor, dass zum behördlichen Datenschutzbeauftragten auch eine Person außerhalb der öffentlichen Stelle bestellt werden kann.

Im Krankenhausbereich werden jedoch regelmäßig sensitive Daten im Sinne des § 3 Abs. 9 LDSG verarbeitet, welche zudem der ärztlichen Schweigepflicht unterliegen (vgl. § 203 Abs. 1 StGB). Da ein externer Datenschutzbeauftragter nicht als Teil der verantwortlichen Stelle im Sinne des § 3 Abs. 3 LDSG anzusehen ist, liegt datenschutzrechtlich eine Übermittlung von Patientendaten vor, wenn dieser im Rahmen seiner Tätigkeit personenbezogene Daten von Patienten zur Kenntnis nimmt. Diese ist nur zulässig, wenn entweder die Einwilligung der Betroffenen oder eine Rechtsvorschrift vorliegt. § 36 Abs. 3 LKG enthält keine Bestimmung, auf die eine solche Datenweitergabe gestützt werden könnte. Auch aus dem Verweis auf das LDSG in § 36 Abs. 8 LKG kann nichts Gegenteiliges abgeleitet werden. Denn mit der Aufgabenstellung eines behördlichen Datenschutzbeauftragten gem. § 11 LDSG ist es grundsätzlich nicht zu vereinbaren, wenn dieser sensitive Daten im Sinne des § 3 Abs. 9 LDSG zur Kenntnis nimmt. Der LfD hat aus diesem Grunde in der Vergangenheit stets die Auffassung vertreten, dass die Kenntnisnahme von geschützten Personaldaten durch den behördlichen Datenschutzbeauftragten ohne Einwilligung des Betroffenen unzulässig ist. Nichts anderes kann im Bereich der Patientendaten durch einen externen Datenschutzbeauftragten gelten.

Auch der Hinweis auf das Verpflichtungsgesetz führt zu keinem anderen Ergebnis. Hierzu ist festzustellen, dass ein externer Datenschutzbeauftragter weder als Berufsgeheimnisträger nach § 203 Abs. 1 StGB noch als Berufsgehilfe im Sinne des § 203 Abs. 3 StGB zu qualifizieren ist. Über das Verpflichtungsgesetz kann lediglich eine strafrechtliche Gleichstellung mit einem Amtsträger nach § 203 Abs. 2 StGB erreicht werden. Die ärztliche Schweigepflicht ist jedoch mit der normalen Schweigepflicht eines Amtsträgers nicht zu vergleichen. In § 203 Abs. 1 und 3 StGB wird die besondere Vertrauensbeziehung zwischen einem Berufsgeheimnisträger und dem Klienten geschützt, welches auch strafprozessual über Zeugnisverweigerungsrechte (vgl. § 53 Abs. 1 Nr. 3 StPO) und Beschlagnahmeverbot (§ 97 StPO) abgesichert ist. Der beamtenrechtlichen Verschwiegenheitspflicht nach § 203 Abs. 2 StGB liegt demgegenüber keine besondere Vertrauensbeziehung zugrunde. Aus diesem Grunde hat der LfD in der Vergangenheit die Auffassung vertreten, dass im vergleichbaren Fall der Auftragsdatenverarbeitung durch Private eine „§ 203 StGB entsprechende Schweigepflicht“ – wie dies § 36 Abs. 9 LKG voraussetzt – über das Verpflichtungsgesetz nicht zu erreichen ist.

Gegen die Beauftragung eines externen privaten Datenschutzbeauftragten im Krankenhausbereich bestehen somit erhebliche datenschutzrechtliche Bedenken.

Zu den Aufgaben und Befugnissen des behördlichen Datenschutzbeauftragten hat der LfD die Orientierungshilfe „Hinweise zum behördlichen Datenschutzbeauftragten“ erstellt, die im Internetangebot des LfD unter der Rubrik „Materialien“ – „Hinweise und Empfehlungen“ abrufbar ist.

10.6.2 Auslagerung der Patientenaktenverwaltung im Krankenhausbereich

Die Beauftragung externer Dritter mit der Verwaltung von Patientenakten gewinnt auch im Krankenhausbereich an Bedeutung. Dies ist nicht ohne Brisanz: sowohl die Vorgaben des Landeskrankenhausgesetzes als auch die Strafandrohung des § 203 Abs. 1 StGB engen die Möglichkeiten einer Auslagerung stark ein. Folgendes ist zu beachten:

Bei dem Führen und Archivieren von Patientenakten handelt es sich aus datenschutzrechtlicher Sicht um die Verarbeitung personenbezogener Daten. Diese Aufgabe obliegt nach § 10 der Berufsordnung für die Ärzte in Rheinland-Pfalz dem jeweiligen behandelnden Arzt. Soweit der Patient in einem Krankenhaus behandelt wird, ist das Krankenhaus nach § 36 Abs. 2 Nr. 1 LKG zur Vornahme der ärztlichen Dokumentation befugt. Soweit Patientenakten automatisiert geführt werden, ist zudem die in § 36 Abs. 7 LKG enthaltene beschränkte Zugriffsberechtigung nach Abschluss der Behandlung zu berücksichtigen.

Ob und in welcher Form die Verarbeitung von Patientendaten aus dem Krankenhausbereich ausgelagert werden kann, richtet sich in Rheinland-Pfalz primär nach § 36 Abs. 9 LKG. Danach kann sich das Krankenhaus zur Verarbeitung von Patientendaten Dritter bedienen, wenn die Einhaltung der Datenschutzbestimmungen des Landeskrankenhausgesetzes sowie eine § 203 StGB entspre-

chende Schweigepflicht beim Auftragnehmer sichergestellt ist. Dies bedeutet, dass es für die Zulässigkeit der angestrebten Auslagerung der Patientenaktenverwaltung entscheidend darauf ankommt, ob der Auftragnehmer seinerseits der ärztlichen Schweigepflicht unterliegt. Zur Wahrung einer § 203 StGB entsprechenden Schweigepflicht reicht eine in diesem Zusammenhang erwogene Verpflichtung von Mitarbeitern des Auftragnehmers nach dem Verpflichtungsgesetz nicht aus (siehe hierzu auch die näheren Ausführungen in Tz. 10.6.1).

Eine organisatorische Einbindung externer Mitarbeiter in das Krankenhaus kann möglicherweise die Vorgaben des § 36 Abs. 9 LKG erfüllen. Ob dies allerdings tatsächlich der Fall ist, hängt von der konkreten Ausgestaltung dieser Einbindung im Einzelfall ab und muss jeweils sorgfältig geprüft werden.

Grundsätzlich sollte im Vorfeld einer angestrebten Auslagerung der Patientenaktenverwaltung, bei der nach § 36 Abs. 1 LKG zumindest dann, wenn es sich um ein in öffentlicher Trägerschaft befindliches Krankenhaus handelt, auch die Vorgaben des § 4 LDSG zu beachten sind, der behördliche Datenschutzbeauftragte des Krankenhauses beteiligt werden.

11. Datenschutz bei Sozialleistungsträgern

11.1 Hartz IV und der Datenschutz

Zu einem deutlich gesteigerten Arbeitsaufkommen im Berichtszeitraum führte die ab dem 1. Januar 2005 anstelle der bisherigen Sozial- bzw. Arbeitslosenhilfe eingeführte Gewährung von Leistungen der Grundsicherung für Arbeitsuchende. Diese unter dem Begriff „Hartz IV“ bekannt gewordene Neuordnung der staatlichen Unterstützung im Bereich der erwerbsfähigen Arbeitslosen veränderte auf der Grundlage des SGB II neben der inhaltlichen Hilfegestaltung gerade auch unter organisatorischen Gesichtspunkten die bislang vorhandenen Behördenstrukturen in erheblichem Maße. Die betroffenen Behörden hatten in kürzester Zeit neben der Bildung einer neuen aus Bundes- und Kommunalverwaltung gespeisten Organisationsform eine funktionierende Infrastruktur bereitzustellen und darüber hinaus die komplizierten gesetzlichen Neuregelungen des SGB II rechtskonform anzuwenden.

Aus datenschutzrechtlicher Sicht kamen mit dem Inkrafttreten des SGB II zahlreiche auch grundsätzliche Fragen auf, die teilweise beantwortet wurden, oftmals aber noch mit dem BfD und den Länderkollegen sowie der BA geklärt werden müssen, und bei denen es zumindest teilweise ungewiss ist, ob man bislang allgemein anerkannten Prinzipien des Datenschutzes wie z. B. dem Erforderlichkeitsgrundsatz, dem Direkterhebungsgrundsatz oder dem Grundsatz der Datenvermeidung und Datensparsamkeit überhaupt gerecht werden kann. Es mag an der Zusammenlegung bisher getrennter Verwaltungsbereiche und der dazugehörenden Verwaltungen liegen, und es mag letztendlich auch wenig Alternativen zu dem eingeschlagenen Weg geben – festzuhalten bleibt, dass mit der im SGB II realisierten Verschmelzung von Leistungs- und Vermittlungsaufgaben der „gläserne Bürger“ ein Stück mehr Wirklichkeit geworden ist. Dies ist zumindest angesichts der derzeit vorhandenen äußerst weitreichenden bundesweiten Recherchemöglichkeiten bei der zum Einsatz kommenden Software aus der Sicht des Datenschutzes zu beklagen.

11.1.1 Entwicklungen auf Bundesebene

Bereits im Vorfeld des Inkrafttretens des SGB II gaben die von der BA im Sommer 2004 veröffentlichten Antragsformulare Anlass zum Tätigwerden. Unter Federführung des BfD überprüfte eine kurzfristig von den Datenschutzbeauftragten gebildete Arbeitsgruppe den 16-seitigen Hauptantrag und die zahlreichen Zusatzblätter und stellte diverse datenschutzrechtliche Mängel fest. Nach Gesprächen mit dem BfD erklärte sich die BA bereit, sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zu erstellen, in denen die meisten der von den Datenschutzbeauftragten bemängelten Punkte klargestellt wurden. Die im September 2004 veröffentlichten Hinweise wurden sowohl den mit der Gewährung des Arbeitslosengeldes II befassten Behörden als auch online den Antragstellern zur Verfügung gestellt. Dennoch erreichten diese Hinweise eine Vielzahl von Antragstellern, die bereits zuvor ihre Anträge eingereicht hatten, nicht mehr. Die 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wies in einer hierzu gefassten Entschließung (vgl. Anlage 10) auf diesen Missstand hin. Mittlerweile hat die BA in Abstimmung mit dem BfD die Antragsvordrucke überarbeitet.

Im Hinblick auf die nach § 44 b Abs. 1 SGB II neu errichteten Arbeitsgemeinschaften war zunächst zwischen dem BfD und den Landesbeauftragten die datenschutzrechtliche Kontrollzuständigkeit zu klären. Angesichts der in § 36 SGB II festgelegten örtlichen Zuständigkeit der Arbeitsgemeinschaften und in Anlehnung an die in § 44 b Abs. 3 SGB II festgelegte Fachaufsicht durch die zuständige oberste Landesbehörde sind diese gemäß § 81 Abs. 3 Satz 1 SGB X regelmäßig als öffentliche Stelle des Landes zu qualifizieren. Sie unterliegen somit der Kontrollzuständigkeit des jeweiligen Landesbeauftragten für den Datenschutz. Ob damit die Arbeitsgemeinschaften auch eigenverantwortlich datenverarbeitende Stelle sind, konnte zwischen den Datenschutzbeauftragten und der BA noch nicht einvernehmlich geklärt werden. Der LfD vertrat bislang die Auffassung, dass mit der Einordnung der Arbeitsgemeinschaften als öffentliche Stellen diese zugleich verantwortliche Stellen i. S. v. § 3 Abs. 3 LDSG werden und den hieraus resultierenden Pflichten wie z. B. der Bestellung eines behördlichen Datenschutzbeauftragten nachkommen müssen.

Weit gravierender für den Datenschutz war und ist der Einsatz des im Zusammenhang mit der Gewährung des Arbeitslosengeldes II zur Datenerfassung und Leistungsberechnung verwendeten Programms A2LL. Das auch von den Arbeitsgemeinschaften in Rheinland-Pfalz genutzte Verfahren, welches nach Wertung des BfD „nicht einmal den datenschutzrechtlichen Basisanforderungen genügt“ (vgl. 20. Tb. des BfD, Tz. 16.1.3), missachtet den Erforderlichkeitsgrundsatz sowie die üblicherweise von den öffentlichen Stellen einzuhaltenden Mindeststandards im technisch-organisatorischen Datenschutz. Die seitens des BfD in seinem 20. Tätigkeits-

bericht ausführlich dargestellten Mängel stellen einen Verstoß gegen das in § 35 SGB I verankerte Sozialgeheimnis dar und wurden dementsprechend von dem BfD förmlich beanstandet. Zugleich forderte die 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der o. g. Entschließung (vgl. Anlage 10) die BA auf, die notwendigen Schritte zur datenschutzgerechten Ausgestaltung des Verfahrens unverzüglich einzuleiten.

Die BA hat inzwischen in Teilbereichen eine Behebung der festgestellten Unzulänglichkeiten – beispielsweise durch Protokollierung der bundesweit möglichen Recherchemöglichkeiten – angekündigt. Zu dem Hauptproblem des Verfahrens, nämlich der bundesweiten Abrufbarkeit sämtlicher erfasster Sozial- und Gesundheitsdaten, ist bislang noch keine technische Lösung erkennbar. Es bleibt abzuwarten, ob, in welchem Maße und insbesondere bis wann den datenschutzrechtlichen Basisanforderungen endlich entsprochen wird.

Zudem erweist sich auch im Zusammenhang mit der Arbeitsvermittlung die gegenwärtig eingesetzte Software als datenschutzrechtlich bedenklich. Es handelt sich hierbei um bislang von der Arbeitsverwaltung genutzte Verfahren (coArb, coLei, coMed, COMPAS), die im Laufe des Jahres 2005 im Rahmen des sog. Virtuellen Arbeitsmarktes von dem Verfahren VerBIS (Vermittlungs-, Beratungs- und Informations-System) abgelöst werden sollen (s. hierzu im Einzelnen 20. Tb. des BfD, Tz. 16.2). Ähnlich dem Verfahren A2LL werden derzeit auch bei der Vermittlung hochsensible Informationen über die Betroffenen erfasst (sog. Vermittlungshemmnisse wie z. B. Gesundheitsbeeinträchtigungen oder Vorstrafen). Aufgrund der fehlenden Zugriffsbeschränkungen können die Mitarbeiter der BA bzw. der Arbeitsgemeinschaften auf sämtliche Daten der Antragsteller und Leistungsbezieher zugreifen, auch wenn sie dies für ihre Aufgabenerfüllung regelmäßig gar nicht benötigen. Der LfD wendet sich dabei keineswegs insgesamt gegen die bundesweite Abrufbarkeit der Daten. Er tritt vielmehr für eine Verfahrensweise ein, bei der – analog zum Krankenhausbereich – nur im Bedarfsfall eine Freischaltung der Datensätze durch die aktenführende Stelle erfolgt.

Ob eine zeitgerechte Ablösung der bisherigen Vermittlungssoftware durch den Virtuellen Arbeitsmarkt tatsächlich realisiert wird und ob das vorgesehene Verfahren VerBIS den Anforderungen des Datenschutzes genügen wird, muss aus heutiger Sicht ebenfalls bezweifelt werden.

11.1.2 Die Situation in Rheinland-Pfalz

Auf der Grundlage des § 44 b SGB II haben auch in Rheinland-Pfalz in weit überwiegendem Maße die betroffenen Leistungsträger (Arbeitsverwaltung und Kommunalverwaltung) zur einheitlichen Wahrnehmung ihrer Aufgaben Arbeitsgemeinschaften gebildet. Lediglich zwei Kreisverwaltungen sind auf der Grundlage des § 6 a SGB II als kommunale Leistungsträger, sog. optierende Kommunen, zugelassen. Der LfD hat im Berichtszeitraum bei zwei Arbeitsgemeinschaften und einer Optionskommune örtliche Feststellungen zum Datenschutz getroffen.

- Anders als bei der Optionskommune wurde bei den Prüfungen der beiden Arbeitsgemeinschaften zunächst festgestellt, dass diese selbst über keinerlei eigene Personalressourcen für die von der BA zur Verfügung gestellte Informationstechnik bzw. die Durchführung administrativer Aufgaben verfügen. Dies betrifft insbesondere die Bereiche Benutzerverwaltung, Pflege von Hard- und Software, Protokollierung/Datensicherheit und User Help Desk. Ansprechpartner waren hierfür Einrichtungen der BA. Ob bzw. welche Zugriffsmöglichkeiten diese Stellen im Hinblick auf den Datenbestand der einzelnen Arbeitsgemeinschaft haben und ob ggf. Protokollierungen dieser Zugriffe erfolgen, blieb offen. Datenschutzrechtlich stellt sich dabei die Frage, auf welcher Grundlage welche Stelle in diesem Zusammenhang tätig wird und inwieweit hierbei personenbezogene Daten durch diese verarbeitet werden. Eine Klärung soll unter Hinzuziehung des BfD und der BA herbeigeführt werden.

- Für eine der kontrollierten Arbeitsgemeinschaften nimmt das von der regionalen Arbeitsagentur betriebene Service-Center telefonische Beratungsdienste wahr. Dieses verfügt für die Beantwortung von Fragen im Zusammenhang mit der Bearbeitung von Anträgen nach dem SGB II über unbeschränkte Zugriffsbefugnisse auf die entsprechenden Fachverfahren, beispielsweise das Programm A2LL. Die datenschutzrechtlichen Rahmenbedingungen einer derartigen Einbindung von Call-Centern in die Aufgabenerledigung der Arbeitsgemeinschaften werden zurzeit abgestimmt.

- Die von einer Arbeitsgemeinschaft zusammen mit der im gleichen Gebäude ansässigen örtlichen Arbeitsagentur vorgesehene Schaffung eines gemeinsamen Empfangsbereiches begegnete im Hinblick auf die dabei angestrebte Einräumung unbeschränkter Zugriffsrechte datenschutzrechtlichen Bedenken. Auch hier bedarf die damit verbundene Übermittlung von Sozialdaten von der Arbeitsgemeinschaft an die Arbeitsagentur einer Rechtsgrundlage. Die Stellungnahme der betroffenen Arbeitsgemeinschaft steht noch aus.

- Im Bereich der Gewährung des Arbeitslosengeldes II kommt es immer wieder zur regelmäßigen Anfertigung und Speicherung von Kopien der von den Betroffenen vorgelegten Kontoauszüge. Dies ist in der Regel nicht erforderlich, sofern sich nicht aus den vorgelegten Unterlagen Abweichungen zu den sonstigen Antragsangaben ergeben. Auch eine Anfertigung von Kopien des Mutterpasses begegnet derartigen Bedenken. Der LfD verwies auf seine Ausführungen zur vergleichbaren Problematik im Sozialhilfeverfahren (vgl. 18. Tb., Tz. 11.6.3).

- Sowohl bei den besuchten Arbeitsgemeinschaften als auch bei der kommunalen Arbeitsagentur wurde die im Zusammenhang mit dem Antrag auf Gewährung eines Mehrbedarfs für kostenaufwändige Ernährung nach § 21 Abs. 5 SGB II ärztlicherseits bestätigte Diagnose – neben weiteren Informationen – elektronisch erfasst und gespeichert.

An der datenschutzrechtlichen Zulässigkeit der Erhebung und insbesondere der Speicherung der Diagnosen der Betroffenen bestehen Zweifel. Der Wortlaut des § 21 Abs. 5 SGB II setzt nicht zwingend die Kenntnis der zugrunde liegenden Erkrankung voraus, sofern der medizinisch notwendige Bedarf der kostenaufwändigen Ernährung durch einen Arzt attestiert wird. Auf jeden Fall ist eine automatisierte Verarbeitung der Diagnoseangabe für die Antragsbearbeitung nicht erforderlich und sollte deshalb unterbleiben. Während die optierende Kreisverwaltung inzwischen mitgeteilt hat, dass die Diagnose aus den Parametern des von der kommunalen Arbeitsagentur eingesetzten Software-Programms entfernt worden sei, steht eine endgültige Klärung der Angelegenheit bezogen auf das von den Arbeitsgemeinschaften benutzte Verfahren A2LL noch aus.

- Im Rahmen der örtlichen Feststellungen stellte sich weiterhin heraus, dass den Mitarbeitern einer kontrollierten Arbeitsgemeinschaft unabhängig von ihrem jeweiligen Einsatzbereich (Antragsbearbeitung Arbeitslosengeld II oder Arbeitsvermittlung) regelmäßig Zugriffsrechte auf sämtliche in der Arbeitsgemeinschaft zum Einsatz kommenden Fachanwendungen wie z. B. A2LL, coArb, coLei, coMed eingeräumt waren. Aufgrund dieser weitgehenden Zugriffsberechtigungen standen den Mitarbeitern bezüglich jedes einzelnen Antragstellers bzw. Betroffenen sehr umfassende Informationsmöglichkeiten sowohl im Hinblick auf dessen Hilfebedürftigkeit als auch hinsichtlich dessen Vermittlungsmöglichkeiten einschließlich der jeweiligen gesundheitlichen Situation zur Verfügung. Dies ist aus datenschutzrechtlicher Sicht angesichts der mit den einzelnen Anwendungen verbundenen bundesweiten Recherchemöglichkeiten selbst bei Vorliegen eines – gegenwärtig – noch nicht vorhandenen Zugriffsberechtigungskonzepts grundsätzlich bedenklich. Auch hier steht die von der Arbeitsgemeinschaft erbetene Stellungnahme zur Erforderlichkeit der eingeräumten sehr weitreichenden Zugriffsbefugnisse noch aus.

- Im Hinblick auf die Datenerhebung für Vermittlungszwecke gehen die geprüften Stellen zumindest nach den bislang gewonnenen Eindrücken sehr uneinheitlich vor. Aus datenschutzrechtlicher Sicht muss in diesem Zusammenhang geklärt werden, welche Informationen von den Betroffenen erhoben werden dürfen und wo – vergleichbar zum Fragerecht des Arbeitgebers im Einstellungsverfahren – Grenzen zu ziehen sind. Dies wird zurzeit zwischen den Datenschutzbeauftragten des Bundes und der Länder diskutiert.

- Die bereits dargestellten datenschutzrechtlichen Mängel der von den Arbeitsgemeinschaften zur Berechnung des Arbeitslosengeldes II bzw. zur Gewährung von Leistungen zur Eingliederung in Arbeit eingesetzten Verfahren bestätigten sich im Rahmen der örtlichen Feststellungen.

11.2 Disease-Management-Programme

Die Durchführung von Disease-Management-Programmen (DMP) und die hierbei zu berücksichtigenden datenschutzrechtlichen Gesichtspunkte waren bereits Gegenstand des 19. Tätigkeitsberichts (Tz. 11.5). Inzwischen sind strukturierte Behandlungsprogramme nicht nur zu Diabetes, sondern auch zu Brustkrebs und zur koronaren Herzkrankheit vereinbart bzw. in der Praxis realisiert.

Die Situation in Rheinland-Pfalz weist in diesem Zusammenhang mehrere Besonderheiten auf: so sind im Lande beide von der Risikostrukturausgleichsverordnung vorgesehenen DMP-Modelle verwirklicht (Abschluss von Kollektivverträgen zwischen Leistungserbringern und Kassenärztlicher Vereinigung unter Beteiligung der Krankenkassen bzw. Abschluss von Einzelverträgen zwischen Leistungserbringern und einer Krankenkasse ohne Beteiligung der Kassenärztlichen Vereinigung). Weiterhin erbringt bundesweit einzigartig im kollektivvertraglichen Modell eine organisatorisch bei der Kassenärztlichen Vereinigung angesiedelte öffentliche Stelle (sog. DMP-Datenstelle) die nach § 28 f Abs. 2 Nr. 1 und 4 RSAV vorgesehenen Datenverarbeitungen.

Im Hinblick auf die den Krankenkassen bei der Durchführung von DMP generell eingeräumten Zugriffsmöglichkeiten auf medizinische Versichertendaten wurde der LfD im Berichtszeitraum um eine allgemeine datenschutzrechtliche Einschätzung gebeten. Im Ergebnis ist aus Sicht des LfD die von dem Gesetzgeber diesbezüglich getroffene Entscheidung akzeptabel: nach den zugrunde liegenden Regelungen der RSAV ist u. a. vorgesehen, dass den Krankenkassen im Rahmen der DMP medizinische Daten der Versicherten übermittelt und von diesen zur Unterstützung der Betreuung des Versicherten verarbeitet und genutzt werden dürfen (§ 28 d Abs. 1 Nr. 3 RSAV). Der Umfang der den Krankenkassen übermittelten Daten bestimmt sich danach, ob die Krankenkasse die Durchführung eines strukturierten Behandlungsprogrammes mit den Kassenärztlichen Vereinigungen oder direkt mit den Leistungserbringern vereinbart hat.

Aus datenschutzrechtlicher Sicht kommt dem Prinzip der informierten Einwilligung, das den strukturierten Behandlungsprogrammen zugrunde liegt, ein besonderes Gewicht zu. Die in § 137 f Abs. 3 SGB V und §§ 28 d u. e RSAV enthaltenen Informationspflichten gegenüber den Versicherten gewährleisten bereits vor der Einschreibung in das Programm einen hohen Grad an Transparenz hinsichtlich der bei der Krankenkasse stattfindenden Datenverarbeitung. Die Versicherten selbst entscheiden dann auf dieser Grundlage, ob sie trotz der mit DMP verbundenen Datenflüsse an die Krankenkasse an dem Programm teilnehmen wollen. Auf der anderen Seite unterliegen die den Krankenkassen im Zusammenhang mit der Durchführung von DMP zulässigerweise überlassenen Versichertendaten einer strengen Zweckbindung (§ 28 d Abs. 1 Nr. 3 RSAV). Kassenintern dürfen zudem nur diejenigen Personen Zugang zu den Dokumentationsdaten haben, die Aufgaben im Rahmen der Betreuung Versicherter in strukturierten Behandlungsprogrammen wahrnehmen und hierfür besonders geschult sind (§ 28 f Abs. 1 Nr. 2 RSAV).

Dem LfD liegen keine Erkenntnisse vor, dass bei den in Rheinland-Pfalz durchgeführten DMP die beteiligten Krankenkassen diesen gesetzlichen Vorgaben nicht entsprechen.

11.3 Sozialdatenschutz gilt auch für Politiker

Es ist nicht Aufgabe des Datenschutzes, die Rechtmäßigkeit der Gewährung von Sozialleistungen zu beurteilen oder zu der Frage Stellung zu nehmen, ob es moralisch vertretbar ist, als sogenannter Besserverdiener Sozialleistungen überhaupt in Anspruch zu nehmen. Das informationelle Selbstbestimmungsrecht ist aber sehr wohl dann betroffen, wenn eine öffentliche Stelle die Presse davon unterrichtet, dass ein Lokalpolitiker – wenn auch gesetzeskonform – Sozialleistungen erhalten hat und dies daraufhin in Zeitungsartikeln als „gierig“ und „Abzocke“ dargestellt wird. Denn die Vorschriften zum Sozialdatenschutz gelten für jeden, auch für Politiker.

Nach der Überzeugung des LfD hatte in dem zu Grunde liegenden Fall eine Kreisverwaltung der Presse Details aus dem Antragsverfahren zugespielt und somit ein wochenlanges Spießrutenlaufen des Betroffenen und seiner Familie mitverursacht. Die Kreisverwaltung stritt eine Datenübermittlung ab; eine Überprüfung der Verfahrensakte durch den LfD ergab jedoch, dass Informationen, welche ausschließlich dem Antragsteller selbst und der Kreisverwaltung bekannt gewesen sein konnten, den Weg in die Presse gefunden hatten. Da der Betroffene selbst als Hinweisgeber auszuschließen war, musste von einer Datenübermittlung durch die Kreisverwaltung ausgegangen werden.

Eine Rechtsgrundlage für diese Informationsweitergabe existierte nicht. Der LfD beanstandete sie daher gegenüber der Kreisverwaltung als Verstoß gegen datenschutzrechtliche Bestimmungen und unterrichtete die Kommunalaufsicht.

11.4 Weitergabe von Sozialdaten an die Führerscheinstelle zur Überprüfung der Fahrtauglichkeit

Mehrfach hatte sich der LfD mit der Frage zu beschäftigen, ob ein Sozialleistungsträger der Führerscheinstelle zulässigerweise mitteilen darf, dass ein Betroffener trotz erheblicher gesundheitlicher Beeinträchtigungen im öffentlichen Straßenverkehr ein Kraftfahrzeug führt.

So wurde etwa dem Sozialamt aus einem zivilrechtlichen Verfahren bekannt, dass ein Betroffener auf dem einen Auge erblindet war und die Sehkraft auf dem anderen Auge nur noch 16% betrug. Der Sozialamtsmitarbeiter wusste jedoch, dass der Betroffene regelmäßig Motorrad fuhr und informierte die Führerscheinstelle über den Sachverhalt. Das Verfahren endete mit dem Entzug der Fahrerlaubnis. Der Anwalt des Petenten vertrat die Auffassung, dass die Datenübermittlung an die Führerscheinstelle wegen Verstoßes gegen das Zweckbindungsgebot rechtswidrig war.

Im Rahmen der datenschutzrechtlichen Bewertung war darauf hinzuweisen, dass nach § 67 d Abs. 1 SGB X eine Übermittlung von Sozialdaten nur dann zulässig ist, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im Sozialgesetzbuch vorliegt. Auf § 69 Abs. 1 SGB X konnte die Informationsweitergabe vorliegend nicht gestützt werden, da die Übermittlung nicht zur Erfüllung eigener Aufgaben nach dem Sozialgesetzbuch erfolgte und sog. fremdnützige Datenübermittlungen lediglich an andere Sozialleistungsträger zulässig sind. Auch die übrigen Übermittlungstatbestände des SGB X waren nicht einschlägig, so dass der LfD zu dem Ergebnis kam, dass die Unterrichtung der Führerscheinstelle nach den Bestimmungen des Sozialgesetzbuchs unzulässig war.

Es ist andererseits nicht von der Hand zu weisen, dass auch die Sozialverwaltung bei einer bestehenden Gefahrenlage nicht tatenlos zusehen, sondern unter Umständen sogar gehalten sein kann, Gefahren für den Betroffenen und für andere Verkehrsteilnehmer abzuwehren. Wenn daher ein Sozialleistungsträger nach sorgfältiger Einzelfallprüfung zu dem Ergebnis gelangt, dass sich aus einer gesundheitlichen Beeinträchtigung des Betroffenen konkrete Gefahren für Leib und Leben Dritter ergeben, hält es der LfD für vertretbar, die Übermittlung der zur Gefahrenabwendung erforderlichen Sozialdaten auf den rechtfertigenden Notstand nach § 34 StGB zu stützen. Da eine strafgesetzliche Vorschrift nach der Auffassung des LfD jedoch nicht dazu dienen kann, eine vermeintlich fehlende Übermittlungsbefugnis zu ersetzen, kommt die Informationsweitergabe an die Führerscheinstelle unter Heranziehung des § 34 StGB nur als Ausnahmetatbestand unter folgenden Voraussetzungen in Betracht:

- Es muss die in § 34 StGB geforderte gegenwärtige, nicht anders abwendbare Gefahr für Leben bzw. Gesundheit Dritter vorliegen. In diesem Zusammenhang ist auch zu klären, ob sich der Betroffene einsichtig verhält oder erklärt, weiterhin Kraftfahrzeuge im öffentlichen Straßenverkehr zu führen. Wurden die medizinischen Informationen von einem Amtsarzt zur Verfügung gestellt, sollte mit diesem Rücksprache gehalten werden, ob aus ärztlicher Sicht eine Unterrichtung der Führerscheinstelle nach Maßgabe des § 11 Abs. 2 Ziff. 3 ÖGDG in Betracht kommt.
- Die Prüfung und Entscheidung, ob die Voraussetzungen des § 34 StGB für eine Unterrichtung der Führerscheinstelle als Ausnahmefall vorliegen, sollte durch eine Person mit Vorgesetztenfunktion getroffen werden, etwa durch den Leiter des Sozialamts oder seinen Stellvertreter.
- Die Voraussetzungen für die Übermittlung und das Verfahren, wie und durch wen sie zu überprüfen sind, sollten den Mitarbeitern des Sozialamtes etwa in Form einer entsprechenden Dienstanweisung bekanntgegeben werden.

Die betroffenen Verwaltungen reagierten auf diese Anforderungen sehr unterschiedlich: Während eine Kreisverwaltung umgehend eine entsprechende Dienstanweisung erließ, weigerte sich eine Verbandsgemeinde aus nicht nachvollziehbaren Gründen hartnäckig, die Rechtsauffassung des LfD anzuerkennen. Unmittelbar vor einer förmlichen Beanstandung konnte letztlich doch noch eine einvernehmliche Lösung erzielt werden.

11.5 Automatisierte Datenverarbeitung im Jugendamt

Wie örtliche Feststellungen bei Kreisverwaltungen in der Vergangenheit gezeigt haben, hat der Vormarsch der automatisierten Datenverarbeitung regelmäßig vor den Türen der Jugendämter Halt gemacht. Offenbar bestand in der Praxis kein sonderlich ausgeprägtes Bedürfnis, die Akte in Papierform durch eine computergestützte Datenverarbeitung abzulösen. Datenschutzrechtlich ist dies keineswegs von Nachteil. Werden etwa die besonders geschützten „anvertrauten Daten" nach § 65 SGB VIII im Jugendamt in einem verschlossenen Behältnis aufbewahrt, entspricht dies den datenschutzrechtlichen Anforderungen. Aber auch die letzte Bastion der Papierdatenverarbeitung innerhalb der Kommunen scheint nunmehr genommen. Denn im Berichtszeitraum vermehrten sich Beratungsanfragen zur automatisierten Datenverarbeitung im Jugendamt.

Aus datenschutzrechtlicher Sicht sollten vor Einführung der automatisierten Datenverarbeitung im Jugendamt die jeweiligen Zugriffsberechtigungen einer eingehenden Prüfung unterzogen werden. Beispielhaft hatte der behördliche Datenschutzbeauftragte einer Kreisverwaltung sämtliche Daten, die künftig automatisiert verarbeitet werden sollen, aufgelistet und in Gesprächen mit den Jugendamtsmitarbeitern geklärt, welcher Mitarbeiter aufgrund seiner Aufgabenzuweisung den Zugriff auf welche Daten benötigt. Die erstellte Übersicht ergab, dass die Bereiche „Allgemeiner Sozialer Dienst" und „Wirtschaftliche Jugendhilfe" gänzlich andere Daten benötigen als beispielsweise die Stellen, die Unterhaltsvorschuss, Pflegekinderdienst und gesetzliche Amtsvormundschaften betreuen. Auf einige Stammdaten war jedoch der Zugriff aller Stellen innerhalb des Jugendamtes erforderlich. Bei erneuter Vorsprache eines Klienten wurde auf Vorschlag des LfD analog zur Regelung im Krankenhausbereich der Zugriff auf bereits vorhandene Daten des Jugendamts von einer vorherigen Freischaltung der aktenführenden Stelle und der Einwilligung des Betroffenen abhängig gemacht. Diese Verfahrensweise ist immer dann sinnvoll, wenn umfassende Zugriffsbefugnisse begehrt werden, um für alle denkbaren Fallkonstellationen gewappnet zu sein. In dem Jugendamt konnte die zum Einsatz kommende Software den datenschutzrechtlichen Anforderungen angepasst werden.

11.6 Interne Organisationsuntersuchungen im Sozial- bzw. Jugendamt

Ob im Rahmen der Durchführung einer verwaltungsinternen Organisationsuntersuchung im Sozial- und Jugendamt auch die ämterübergreifende Weitergabe personenbezogener Daten zulässig ist, war Gegenstand einer an den LfD gerichteten Anfrage einer Kreisverwaltung. Dabei war zu berücksichtigen, dass im konkreten Fall die von dem Organisationsamt der Kreisverwaltung beabsichtigte Untersuchung im Unterschied zu den zu Rechnungsprüfungszwecken durchgeführten Prüfungen der Rechnungsprüfungsbehörden ausschließlich der Verbesserung der inneren behördlichen Organisation dienen sollte.

Grundsätzlich gelten nach § 14 Abs. 6 LDSG auch bei einer Weitergabe personenbezogener Daten innerhalb einer verantwortlichen Stelle die materiellen Regelungen zur Übermittlung personenbezogener Daten, d. h. vorbehaltlich einer § 14 LDSG verdrängenden bereichsspezifischen Norm ist eine solche behördeninterne Übermittlung nur zulässig, wenn dies für die Durchführung der Organisationsuntersuchung erforderlich ist (§ 14 Abs. 1 i. V. m. § 12 Abs. 4 Nr. 6 LDSG).

Soweit die Organisationsuntersuchungen im Sozial- und Jugendamt der Kreisverwaltung durchgeführt werden sollen und demzufolge in erster Linie Sozialdaten betroffen sind, richtet sich die Zulässigkeit der Datenübermittlung an das Organisationsamt nach den §§ 67 d ff. SGB X. Nach § 69 Abs. 5 SGB X i. V. m. § 67 c Abs. 3 Satz 1 SGB X ist die Übermittlung von Sozialdaten an die Organisationseinheit, die zur Durchführung von Organisationsuntersuchungen in der verantwortlichen Stelle zuständig ist, grundsätzlich zulässig. Begrenzt wird diese Übermittlungsbefugnis allerdings durch den Grundsatz der Erforderlichkeit (§ 69 Abs. 1 SGB X), d. h. die angestrebte Datenübermittlung an das Organisationsamt muss zur Durchführung der Organisationsuntersuchung auch erforderlich sein. Konkret bedeutet dies, dass vor der beabsichtigten Übermittlung zu prüfen ist, ob es zur Durchführung des Prüfungsauftrags nicht genügt, anonymisierte Aktenteile bzw. anonymisierte Kopien aus Akten zu verwenden. Gerade angesichts des in § 78 b SGB X enthaltenen Grundsatzes der Datenvermeidung und Datensparsamkeit sollte regelmäßig das Ziel verfolgt werden, so wenig Sozialdaten wie möglich zu verarbeiten. Sofern dennoch aus Sicht des Organisationsamtes eine Übermittlung personenbezogener Daten erforderlich sein sollte, wäre dies zu begründen.

Zu beachten ist darüber hinaus, dass das SGB VIII für den Bereich der Jugendhilfe ebenfalls Vorschriften über die Verarbeitung von Sozialdaten enthält, die den allgemeinen Regelungen des SGB X vorgehen. Angesichts des in § 65 SGB VIII enthaltenen besonderen Vertrauensschutzes anvertrauter Daten kommt deren Übermittlung an das Organisationsamt zum Zwecke der Organisationsuntersuchung nicht in Betracht.

11.7 Videoüberwachung in einem Sozialamt

Bei der datenschutzrechtlichen Beurteilung der von einer Kommunalverwaltung beabsichtigten Videoüberwachung innerhalb eines Sozialamtes war zwischen dem erhöhten Sicherheitsbedürfnis der Behördenmitarbeiter einerseits und dem besonderen Schutz der Sozialdaten andererseits abzuwägen.

Im konkreten Fall hatte die Stadtverwaltung vor, zur Verhinderung von gewalttätigen Übergriffen den Flur des betroffenen Sozialamtes, der gleichzeitig auch als Wartebereich dient, mittels einer Videokamera zu beobachten und bei konkreten Anhaltspunkten für bevorstehende möglicherweise gewalttätige Handlungen einzelner Besucher die Mitarbeiter zu warnen bzw. sofort Hilfe herbeizuholen. Die ausschließlich einem leitenden Mitarbeiter des Sozialamtes zugänglichen Videoaufnahmen sollten nicht aufgezeichnet werden. Obwohl die Kamera selbst nicht über eine Zoomfunktion verfügte, war davon auszugehen, dass die von der Be-

obachtung betroffenen Personen in den meisten Fällen erkennbar sind. Dem Vorhaben lagen diverse Vorfälle in der Vergangenheit zugrunde, bei denen städtische Mitarbeiter durch Besucher des Sozialamtes bedroht bzw. körperlich z. T. erheblich verletzt wurden. Die von den Mitarbeitern gewünschte Überwachung sollte der Gefahr künftiger Übergriffe nun wirksam begegnen.

Auch wenn der LfD einem zunehmendem Einsatz von Videokameras durch öffentliche Stellen und insbesondere der Überwachung behördeninterner Räumlichkeiten äußerst zurückhaltend gegenübersteht, war die Durchführung des o. g. von der Stadtverwaltung ins Auge gefassten Vorhabens aus datenschutzrechtlicher Sicht noch vertretbar. Neben der im konkreten Fall aus der eingesetzten Technik resultierenden relativ geringen Eingriffsintensität der Maßnahme sprachen insbesondere deren breite Akzeptanz bei den Mitarbeitern und die von dem Arbeitgeber grundsätzlich zu beachtenden Fürsorgeaspekte zugunsten Bediensteter, die in besonders gefährdeten Verwaltungsbereichen eingesetzt werden, für die Zulässigkeit der Überwachung. In der Gesamtabwägung traten hier die zweifellos von der Maßnahme betroffenen und bedeutsamen Gesichtspunkte des Sozial- und Personaldatenschutzes bei Einhaltung der in § 34 LDSG enthaltenen Voraussetzungen zurück.

Es bleibt festzuhalten, dass der LfD mit der getroffenen Bewertung keine grundsätzliche Akzeptanz verwaltungsinterner Videoüberwachungsvorhaben signalisieren möchte. Die datenschutzrechtliche Zulässigkeit derartiger Maßnahmen hängt immer von den Umständen des Einzelfalls ab und muss jedesmal gesondert festgestellt werden. Neben der obligatorischen Einschaltung des behördlichen Datenschutzbeauftragten sollte deshalb – nicht zuletzt angesichts der Regelungen der §§ 9 Abs. 5, 27 Abs. 1 LDSG – vor Beginn solcher Videobeobachtungen auch der LfD unterrichtet werden.

11.8 Datenschutz in Kindertagesstätten

Der Entwurf des Landesgesetzes zum Ausbau der frühen Förderung (LT-Drs. 14/4453) sieht vor, dass die Beobachtung und Dokumentation der kindlichen Entwicklungsprozesse flächendeckend verbindlich eingeführt werden soll.

Es ist von großer datenschutzrechtlicher Relevanz, wenn künftig für jedes in einer Kindertagesstätte betreute Kind das Führen einer Bildungs- und Lerndokumentation, mithin einer personenbezogenen Akte, gesetzlich vorgeschrieben wird. Hier gilt es zu verhindern, dass sich ein Kind im späteren Leben einmal vorhalten lassen muss, dass es als Vierjähriges noch Windeln benötigte oder wiederholt Spielkameraden mit Bauklötzen traktierte.

Es ist aus Sicht des LfD zu begrüßen, dass eine tragfähige rechtliche Grundlage für das Vorhalten einer Bildungs- und Lerndokumentation geschaffen werden soll und dass die Beachtung des Datenschutzes im Gesetz selbst Erwähnung findet. Allerdings hält er es für erforderlich, dieses allgemeine Postulat näher zu konkretisieren, da nach seinen Erfahrungen in der Praxis angesichts der vielfältigen bundes- und landesrechtlichen Bestimmungen Verunsicherungen, mitunter auch Unkenntnis, in Bezug auf die datenschutzrechtlichen Anforderungen bestehen.

Der LfD hat daher vorgeschlagen, folgende Rahmenbedingungen zum Führen der Bildungs- und Lerndokumentationen an geeigneter Stelle verbindlich festzuschreiben:

- Unterrichtung der Erziehungsberechtigten über das Führen der Bildungs- und Lerndokumentation,
- Information der Erziehungsberechtigten über ihr Einsichtsrecht,
- enge Zweckbindung der Dokumentation (Verbot der Weitergabe von personenbezogenen Daten an Dritte ohne schriftliche Einwilligungserklärung der Eltern),
- Löschungsverpflichtung bei Verlassen der Einrichtung bzw. Herausgabe der Dokumentation an die Erziehungsberechtigten,
- Regelung, dass nach Verlassen der Einrichtung ein weiteres Vorhalten der Bildungs- und Lerndokumentation für Qualitätssicherungszwecke lediglich in anonymisierter Form zulässig ist.

Darüber hinaus nahm der LfD zu Fragen des Informationsaustauschs zwischen Grundschule, Kindergärten und Jugendhilfe sowie zu Fragen der Qualitätssicherung Stellung. Das MBFJ signalisierte Bereitschaft zur Umsetzung der datenschutzrechtlichen Anforderungen. Der LfD wird den Gang des Gesetzgebungsverfahrens auch weiterhin kritisch begleiten.

12. Datenschutz im Ausländerwesen

12.1 Schengener Informations-System (SIS)

Die Gemeinsame Kontrollinstanz zum Schutz personenbezogener Daten (GKI) hatte Anfang 2004 von einer sehr unterschiedlichen Ausschreibungspraxis bei den einzelnen Schengen-Vertragsparteien berichtet, obwohl alle Ausschreibungen auf der Grundlage des Art. 96 des Schengener Durchführungsübereinkommens (SDÜ) erfolgt waren. Zur Harmonisierung der Ausschreibungsvoraussetzungen und -verfahren regte die GKI in allen Vertragsstaaten eine koordinierte Prüfung der datenschutzrechtlichen Zulässigkeit von Speicherungen im SIS an. Der Bundesbeauftragte für den Datenschutz griff im März 2004 die Empfehlung der GKI auf und startete unter Einbeziehung aller Bundesländer eine Kontrolle des Ausschreibungsverfahrens von Personen, die nicht Staatsangehörige eines der Mitgliedstaaten der Europäischen Gemeinschaften sind. Nach einem Zufallsgenerator (jede 500. Ausschreibung) ausgewählt, untersuchten die jeweils zuständigen Datenschutzaufsichtsbehörden ungefähr 400 Ausschreibungen. Um ein weitgehend gleichmäßiges Prüfverfahren sicherzustellen, wurden anhand eines abgestimmten Fragebogens die Rheinland-Pfalz zugeleiteten Prüffälle (insgesamt 17 Fälle bei zehn Ausländerbehörden) einer datenschutzrechtlichen Kontrolle unterzogen. Resümie-

rend war bei der multilateralen Kontrolle, die zum 1. Juni 2004 ihren Abschluss fand, für Rheinland-Pfalz festzustellen, dass ca. ein Drittel der geprüften Akten keine Anhaltspunkte für Verstöße gegen datenschutzrechtliche Bestimmungen aufwies, bei etwa zwei Dritteln der Akten hingegen schlossen sich die Ausländerbehörden der vom LfD empfohlenen Löschung wegen unzureichender Rechtsgrundlage (Ausschreibung ausschließlich aufgrund des „Abtauchens“ der Asylbewerber) oder Ablaufs der Aufbewahrungsfristen an.

12.2 Zulässigkeit von Datenerhebungen bei der Erteilung einer Aufenthaltserlaubnis

Einige Ausländerbehörden hatten im Rahmen des Verfahrens zur Erteilung von Aufenthaltsberechtigungen Fragebögen eingesetzt, die eine Erhebung besonderer Arten personenbezogener Daten im Sinne des § 3 Abs. 9 LDSG vorsahen. Nach Auffassung des LfD bedarf die Erhebung derart sensibler Daten einer besonderen Würdigung des Erforderlichkeitsgebots, denn die Erhebung von Daten wie beispielsweise von Krankheiten, Volkszugehörigkeit und Religion ist nach § 86 Satz 2 AufenthG nur zulässig, „soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist“. Zwar ist es denkbar, in begründeten Einzelfällen Daten zu gefährlichen, ansteckenden Krankheiten bzw. zur Reisefähigkeit zu erheben. Wenn solche Daten aber mittels eines Vordrucks generell unterschiedslos und undifferenziert bei allen Antragstellern erhoben werden, widerspricht dieses Verfahren den gesetzlichen Regelungen im Aufenthaltsgesetz. Dieser Auffassung schloss sich auch das ISM an und informierte die Ausländerbehörden mittels eines inhaltlich mit dem LfD abgestimmten Schreibens. Danach ist die routinemäßige Erhebung von Daten, die im Sinne des § 3 Abs. 9 LDSG als besonders schützenswert anzusehen sind, nicht zulässig.

12.3 Übermittlung personenbezogener Daten an ausländische Behörden zwecks Ausstellung von Passersatzpapieren

Eine Kreisverwaltung ersuchte den LfD vor dem Hintergrund der Abschiebung eines iranischen Ausreisepflichtigen um Prüfung der Zulässigkeit der bisher von rheinland-pfälzischen Ausländerbehörden praktizierten Verfahrensweise bei der Passersatzbeschaffung zur Rückführung undokumentierter Ausländer.

Der LfD hat die Auffassung vertreten, dass Ausländer, die sich in der Bundesrepublik Deutschland aufhalten, nach deutschem Recht unter bestimmten Voraussetzungen verpflichtet sind, an Verwaltungsverfahren auch ausländischer Behörden mitzuwirken. Die Pflicht, die zur Beschaffung der für die Abschiebung notwendigen Reisedokumente unverzüglich beizubringen, ergab sich zum Zeitpunkt der Beurteilung aus §§ 70 Abs. 1 Satz 1 AuslG, 15 Abs. 2 Nr. 6 AsylVfG. Bei mündlichen oder schriftlichen Befragungen zum Zwecke der Feststellung der vermuteten Staatsangehörigkeit handelt es sich jedoch nicht um ein deutsches, sondern ein ausländisches Verwaltungsverfahren. Denn nicht die Vorbereitung und der Erlass eines Verwaltungsaktes gemäß § 9 VwVfG ist Zweck der Maßnahme, sondern die Beseitigung eines praktischen Vollzugshindernisses bei der Abschiebung. Zuständig für die Ausstellung seiner eigenen Reisedokumente ist der jeweilige ausländische Staat. Somit findet das deutsche Verwaltungsverfahrensrecht keine Anwendung bei der schriftlichen oder mündlichen Befragung ausreisepflichtiger ausländischer Personen.

Zweifellos kann aber die Beschaffung von Heimreisedokumenten nicht nur als eine innere Angelegenheit zwischen dem Ausländer und seinem Heimatstaat gesehen werden. Aus der Sicht des LfD kommt deutschen Ausländerbehörden eine besondere Fürsorgepflicht zu, die sich insbesondere auf die Anwendung des Erforderlichkeitsgrundsatzes hinsichtlich der für die Passbeschaffung notwendigen Daten erstreckt. So sollten die Antragsformulare beispielsweise keine Fragen enthalten, die auf eine Asylantragstellung schließen lassen, die Anforderungen an den Nachweis oder die Glaubhaftmachung der Staatsangehörigkeit des betroffenen Personenkreises auf einem möglichst niedrigen Level gehalten und die Betroffenen darauf hingewiesen werden, dass sie keinerlei Angaben machen müssen, die zur Passersatzbeschaffung nicht unbedingt erforderlich sind. Nicht unerwähnt bleiben sollte, dass bei der breiten Palette der Passbeschaffungsmaßnahmen Fallkonstellationen (wie beispielsweise bei totaler Mitwirkungsverweigerung) denkbar sind, bei denen es zu Datenübermittlungen an ausländische Vertretungen kommen kann. Es bestehen dann keine Bedenken gegen eine Übermittlung, wenn es sich ausschließlich um die zur Passbeschaffung notwendigen Daten handelt, die dem Herkunftsstaat ohnehin vorliegen. Mit Blick auf den in § 17 Abs. 3 Nr. 4 LDSG enthaltenen Rechtsgedanken kann dem ausländischen Staat die Möglichkeit der Prüfung, ob es sich bei dem Betroffenen um einen eigenen Staatsangehörigen handelt, nicht vorenthalten werden, insbesondere wenn Betroffene aktiv gegen ausländerrechtliche Bestimmungen (§ 70 Abs. 1 AuslG) verstoßen.

Die bisher von der rheinland-pfälzischen Clearingstelle praktizierte Verfahrensweise – die Passersatzbeschaffung für den iranischen Asylbewerber eingeschlossen – hat auch unter Zugrundelegung dieser Anforderungen keine Verstöße gegen datenschutzrechtliche Regelungen erkennen lassen.

13. Datenschutz in der Finanzverwaltung

13.1 Zentrales Konteninformationssystem

Aufgrund des „Gesetzes zur Förderung der Steuerehrlichkeit“ erhalten ab dem 1. April 2005 aufgrund § 93 Abs. 7 und 8 AO eine Vielzahl von Behörden Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 vorgehalten werden müssen. Dabei handelt es sich um die Stammdaten der Bankkunden, wie Name, Geburtsdatum, Anzahl und Nummern der Konten. Die von den Banken seit 2003 zum Abruf bereitgestellten Daten dienen ursprünglich der Bekämpfung illegaler Finanztransaktionen.

Nach dem neuen Gesetz können Finanzbehörden und andere öffentliche Stellen über das Bundesamt für Finanzen bei den Kreditinstituten Informationen über die Konten bestimmter Bankkunden erhalten. Voraussetzung für eine Abfrage ist, dass die anfra-

gende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes anknüpft“ und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Um welche Begriffe es sich dabei handelt, ist nicht abschließend definiert. Da das Einkommensteuerrecht eine Vielzahl von Begriffen verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), war völlig unklar, welche Behörden die Abfrageberechtigung erhalten. Zudem wurde nicht deutlich, welche Zwecke eine Abfrage rechtfertigen sollen. Von der Tatsache des Abrufs erfahren das Kreditinstitut und der Betroffene zunächst nichts.

Auf diese fehlende Normenklarheit und die unzureichende Information der Betroffenen über den Abruf hatten die Datenschutzbeauftragten des Bundes und der Länder bereits während des Gesetzgebungsverfahrens im Herbst 2003 aufmerksam gemacht. Ihre Forderungen haben sie nochmals in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. Anlage 11) wiederholt.

Das Bundesverfassungsgericht lehnte den Erlass einer einstweiligen Anordnung gegen das In-Kraft-Treten des § 93 Abs. 7 und 8 AO mit seinen Beschlüssen vom 22. März 2004 ab. Das Gericht betonte aber ausdrücklich, dass der Ausgang des Verfahrens in der Hauptsache offen sei. Seine Entscheidung hat es insbesondere darauf gestützt, dass das Bundesfinanzministerium kurz zuvor in einem Anwendungserlass zu den umstrittenen Regelungen die näheren Voraussetzungen für deren Umsetzung festgelegt hatte. So ergibt sich aus dem Anwendungserlass abschließend, welche Behörden Kontodaten abrufen dürfen. Auch wird bestimmt, dass die Betroffenen bereits im Vorhinein auf die Möglichkeit des Abrufs aufmerksam gemacht und nach dem Abruf ebenfalls informiert werden. Ebenso wird das Verfahren formalisiert und somit eine Dokumentation des Abrufersuchens sichergestellt. Damit kommt zumindest der Anwendungserlass den grundsätzlichen Forderungen der Datenschutzbeauftragten nach. In ihren Stellungnahmen zu den Verfassungsbeschwerden haben die Datenschutzbeauftragten des Bundes und der Länder gefordert, die im Anwendungserlass enthaltenen Konkretisierungen im Gesetz selbst zu regeln. Dies ist verfassungsrechtlich geboten.

13.2 Elektronische Umsatzsteueranmeldungen

Ab dem 1. Januar 2005 dürfen die Steueranmeldungen nach Einkommensteuer- und Umsatzsteuergesetz nur noch auf elektronischem Weg nach Maßgabe der Steuerdatenübermittlungsverordnung (StDÜV) an das Finanzamt übermittelt werden. Dazu kann die kostenlose ELSTER-Software (ELSTER = Elektronische Steuererklärung) genutzt werden. Eine Authentifizierung der Steuerbürger wäre eigentlich nach der Abgabenordnung durch den Einsatz einer qualifizierten elektronischen Signatur zu gewährleisten. Jedoch soll hierauf unter den Voraussetzungen des § 6 Abs. 1 StDÜV verzichtet werden und ein anderes geeignetes Authentifizierungsverfahren eingerichtet werden. Ein solches stand jedoch noch nicht ab dem 1. Januar 2005 zur Verfügung. Dies erleichterte Manipulationen, was aus datenschutzrechtlicher Sicht bedenklich ist. Sowohl der Bundesbeauftragte als auch die Landesbeauftragten für den Datenschutz dringen daher auf eine rasche Lösung der Authentifizierungsfrage. Die Finanzverwaltung ermöglicht noch für eine Übergangszeit die Steueranmeldung in schriftlicher Form, teilt im Übrigen die datenschutzrechtlichen Bedenken allerdings nicht. Auch auf anderem Wege könne es zu Manipulationen kommen, die in der Regel stets aufgedeckt würden, so dass die Betroffenen zu viel gezahlte Steuerbeträge zurückerhielten. Ein Authentifizierungsverfahren werde voraussichtlich ab 2006 bundesweit eingeführt.

13.3 Meldedatenübermittlung zur Vorbereitung der Steueridentifikationsnummer

Die Abgabenordnung sieht in § 139 a vor, dass jedem Steuerpflichtigen – demnächst – eine eindeutige Identifikationsnummer zugeordnet wird. Dafür sollen bestimmte Daten aus den Melderegistern an das Bundesamt für Finanzen übermittelt werden ab dem Zeitpunkt, ab dem eine Rechtsverordnung den Start für die Vergabe der Identifikationsnummer festlegt. Eine solche Festlegung erfolgte noch nicht. Dennoch möchte das Bundesamt für Finanzen bereits jetzt die genannten Meldedaten haben. Denn man will im Vorfeld „Testläufe“ durchführen. Dabei geht es insbesondere darum, die Melderegister der einzelnen Länder miteinander abzugleichen, um Fehler bereits im Vorfeld aufzudecken und zu beheben.

Eine Datenübermittlung auf Grundlage der AO kommt nicht in Betracht, da die erforderliche Rechtsverordnung noch nicht erlassen wurde. Bei einer Übermittlung der Meldedaten besteht die Gefahr, dass zumindest für eine Übergangszeit ein zentrales Melderegister beim Bundesamt für Finanzen entsteht, was auf erhebliche datenschutzrechtliche Bedenken stößt. Eine entsprechende Übermittlung würde auch nur Sinn machen, wenn gleichzeitig alle Länder ihre Meldedaten in einheitlicher Form zur Verfügung stellen würden, um den Abgleich auf Grundlage aktueller und vollständiger Datensätze durchführen zu können. Da die Melderegister ganz unterschiedlich geführt werden, dürften diese Voraussetzungen nur schwer zu erfüllen sein. Auch wurde überlegt, eine Datenübermittlung im Wege der Datenverarbeitung im Auftrag durchzuführen: Das Bundesamt für Finanzen wird beauftragt, die rheinland-pfälzischen Meldedaten zu konsolidieren. Es erscheint jedoch fraglich, ob eine solche Konstruktion zulässig ist. Insbesondere ist unklar, in welcher Weise ein Datenabgleich durchgeführt werden soll.

13.4 Auftragsdatenverarbeitung im Gebührenbereich

Viele Kommunen sind finanziell und personell nicht mehr in der Lage, ihre Gebührenbescheide selbst zu erstellen und zu versenden. Dies erfordert für sie in der Regel die Anschaffung von teuren Maschinen, die dann nur temporär zum Einsatz kommen. Deswegen stehen die hohen Anschaffungskosten in keinem angemessenen Verhältnis zur Nutzung. Dies führt dazu, dass der Druck und Versand von Gebührenbescheiden an externe Dienstleister vergeben wird. Dies ist dann unproblematisch, wenn ein Dienst-

leister in öffentlicher Trägerschaft, z. B. ein kommunales Rechenzentrum, den Auftrag erhält. An gesetzliche Grenzen stößt man jedoch bei der Vergabe an private Anbieter: Für kommunale Gebühren, wie Abfallgebühren, Schmutzwassergebühren oder auch Kurbeiträge, gilt gem. § 3 Abs. 1 Nr. 1 KAG i. V. m. § 30 AO das Steuergeheimnis. Dies steht gem. § 4 Abs. 4 Satz 2 LDSG grundsätzlich einer Auftragsdatenverarbeitung durch nicht-öffentliche Stellen entgegen. Danach soll an nicht-öffentliche Stellen ein Auftrag zur Datenverarbeitung nur vergeben werden, wenn überwiegende schutzwürdige Interessen, insbesondere Berufs- oder besondere Amtsgeheimnisse, nicht entgegenstehen. Danach ist das Erstellen und Versenden von Gebührenbescheiden durch ein privates Unternehmen nur ausnahmsweise zulässig. Von einer Ausnahmesituation kann z. B. unter den o. g. Voraussetzungen ausgegangen werden, nämlich dann, wenn die zuständige Kommune personell oder finanziell nicht in der Lage ist, die Bescheide selbst zu erstellen und auch kein öffentlich-rechtliches Unternehmen für die Durchführung dieser Aufgabe unter akzeptablen Bedingungen in Betracht kommt. Vertraglich muss dann festgelegt werden, dass sich der Auftragnehmer der Aufsicht des LfD unterwirft und dass die Mitarbeiter des Auftragnehmers durch den Auftraggeber auf das Steuergeheimnis verpflichtet werden. Weiterhin ist zu dokumentieren, welche Daten auf welchem Weg zum Auftragnehmer gelangen und wie sie dort verarbeitet und schließlich vernichtet oder zurückgegeben werden. Der LfD hatte im Berichtszeitraum Gelegenheit, sich einige private Dienstleister im Rahmen seiner Prüftätigkeit anzusehen. Aufgrund dieser Erfahrungen ist davon auszugehen, dass private Firmen aus datenschutzrechtlicher Sicht ebenso zuverlässig arbeiten wie öffentliche Auftragnehmer.

13.5 Haben Sie eine Seidentapete?

Im Rahmen der Einheitsbewertung des Grundbesitzes verschicken die Finanzämter Fragebögen, in denen sehr detaillierte Auskünfte zur Ausstattung des Grundbesitzes gemacht werden sollen. So soll z. B. angegeben werden, ob der Grundbesitz Eichenholztüren, Edelholztüren oder Schleiflacktüren hat oder ob Decken und Wände mit Seidentapeten, Stoff- oder Lederbespannung oder gar Deckenmalerei versehen sind. Dies erscheint zunächst ein sehr intimer Einblick in die Privatsphäre der Steuerpflichtigen zu sein. Eine Überprüfung hat jedoch ergeben, dass dieses Verfahren datenschutzrechtlich nicht zu beanstanden war: Bei der Berechnung der Grundsteuer ist gem. § 13 Abs. 1 Grundsteuergesetz von einem Steuermessbetrag auszugehen. Dieser ist durch Anwendung eines Tausendsatzes (Steuermessteil) auf den Einheitswert oder seinen steuerpflichtigen Teil zu ermitteln, der nach dem Bewertungsgesetz im Veranlagungszeitpunkt für den Steuergegenstand maßgebend ist. Der maßgebende Grundstückswert ist nach den Vorgaben des Bewertungsgesetzes festzusetzen. Dieses Gesetz kennt zur Ermittlung des gemeinen Wertes von bebauten Grundstücken auf der Basis der Wertverhältnisse vom 1. Januar 1964 zwei Verfahren: Das Ertragswertverfahren (§ 78 ff. Bewertungsgesetz) und das Sachwertverfahren (§§ 83 ff. Bewertungsgesetz). Der fragliche Vordruck war für Fälle des Ertragswertverfahrens vorgesehen und diente der Bestimmung des Vervielfältigers (§ 80 Bewertungsgesetz) und der üblichen Miete (§ 79 Bewertungsgesetz), aber auch der Entscheidung, ob ggf. das Sachwertverfahren anzuwenden ist (§ 76 Bewertungsgesetz).

Nach dem Ertragswertverfahren wird der Grundstückswert gem. § 78 Bewertungsgesetz durch Anwendung eines Vervielfältigers auf die Jahresrohmiete festgelegt. Folglich müssen im Ertragswertverfahren die Jahresrohmiete sowie der Vervielfältiger ermittelt werden. Für den Vervielfältiger sind gem. § 80 Abs. 1 Bewertungsgesetz Grundstücksart, Bauart, Bauausführung, Baujahr und die Einwohnerzahl der Gemeinde maßgebend. Für die Festsetzung der Jahresrohmiete muss die Ausstattung des fraglichen Grundeigentums erfasst werden. Nach den Ausführungen der Oberfinanzdirektion Koblenz waren die im fraglichen Formular erfassten Daten hierzu zwingend notwendig. Bei der Bestimmung der üblichen Miete und auch des Raummeterpreises kam es auf die Summe der wertbildenden Faktoren an, bei der auch innerhalb der gleichen Ausstattungsstufe das jeweilige Einzelmerkmal gewichtet werden musste.

14. Wirtschaft und Verkehr

14.1 Portal Gewerbemeldungen

Das Statistische Landesamt ist mit einem Projekt zur Verwaltungsvereinfachung an den LfD herangetreten. Es handelt sich um ein zu schaffendes Portal, über das die Städte und Gemeinden Mitteilungen über Gewerbemeldungen an die Institutionen übermitteln können, die diese Daten aufgrund der Bestimmung in § 14 Abs. 5 GewO regelmäßig erhalten. Hierzu gehören z. B. die Industrie- und Handelskammern, Finanzämter, Umweltämter, die Berufsgenossenschaften oder die Eichämter. Da bei diesem Verfahren personenbezogene Daten übermittelt werden, wurde der LfD um Stellungnahme gebeten.

Bislang wird für den Verteilprozess in der Regel ein 11fach-Durchschreibesatz verwendet. Die Gewerbeämter müssen gegenwärtig, obwohl sie selbst EDV-Programme für die Erfassung der Gewerbemeldungen nutzen, in Papierform – grundsätzlich per „gelber Post“ – verschiedene Datenbestände mit großem manuellen Aufwand an die zuständigen unterschiedlichen Stellen liefern. Diese wiederum müssen die Daten nochmals erfassen, um sie in den eigenen IT-Systemen weiterverarbeiten zu können. Mit dieser Form der Datenverarbeitung soll nun Schluss sein.

Es ist vorgesehen, die erforderlichen Daten ohne Medienbruch als Datei an einen zentralen Datenbankserver zu senden. Dieser soll die Daten entsprechend den Vorschriften der Gewerbeordnung auf die einzelnen Nutzer verteilen und sie darüber informieren, wenn neue Daten zur Verfügung stehen. Die Nutzer könnten sie dann entsprechend herunterladen und direkt in ihre Systeme einspielen. In diesem Zusammenhang würde das Statistische Landesamt Rheinland-Pfalz die Benutzerdaten verwalten, wobei der zentrale Server vom hessischen Statistischen Landesamt vorgehalten werden soll.

Rechtlich gesehen findet hier eine Auftragsdatenverarbeitung im Anwendungsbereich des § 4 LDSG statt. Auftraggeber sind die jeweiligen Kommunen, die von den Möglichkeiten dieses Verfahrens Gebrauch machen möchten. Auftragnehmer ist das Statistische Landesamt, das mittels Administration der Benutzerdaten dafür Sorge trägt, dass die Gewerbeanzeigen im Auftrag der angeschlossenen Kommunen verteilt werden. Dieses begründet seinerseits ein Unterauftragsverhältnis mit dem hessischen Statistischen Landesamt, um den dort vorgehaltenen zentralen Server (der im Gewerbemeldeverfahren den hessischen Kommunen bereits als „Drehscheibe“ dient) zu nutzen.

Um projektbezogen eine datenschutzgerechte Handhabung zu gewährleisten, sind zunächst grundsätzliche Fragen zu klären, was die Rechte und Pflichten von Auftraggeber und Auftragnehmer anbelangt. Dies müsste im Einzelnen in einem entsprechenden Vertrag im Sinne von § 4 Abs. 2 LDSG festgelegt werden. Von besonderer Bedeutung ist es sicherzustellen, dass die seitens der Kommunen auf den Server übertragenen Daten dort in einem abgeschotteten, physikalisch getrennten Bereich vorgehalten werden. Des Weiteren bedarf die zu Administrationszwecken einzurichtende Netzverbindung zwischen Bad Ems – dem Sitz des Statistischen Landesamtes – und Wiesbaden einer Regelung hinsichtlich der Leitungssicherheit. Auf dieser Strecke sollte entsprechend der Verfahrensweise im rlp-Netz verschlüsselt übertragen werden.

Sofern sich das Vorhaben weiter konkretisiert, wird eine gemeinsame Erörterung der Detailfragen stattfinden.

14.2 Veröffentlichung des Gewerberegisters der Verbandsgemeinde im Internet?

Eine Verbandsgemeinde bat den LfD um seine Einschätzung zu der Überlegung, die dort im Gewerberegister gemeldeten Gewerbetreibenden mit den Grunddaten „im Internet einstellen zu lassen“.

Er hat darauf hingewiesen, dass damit jedermann in die Lage versetzt würde, entsprechende Auskünfte aus dem Gewerberegister voraussetzungslos zu erhalten. Die einschlägigen Übermittlungsregelungen finden sich in § 14 Abs. 6 und 8 GewO. Dort wird hinsichtlich der Angaben über Name, betriebliche Anschrift und ausgeübte Tätigkeit des Gewerbetreibenden – die drei Grunddaten aus einer Gewerbeanzeige – bei öffentlichen Stellen (Abs. 6) auf die Erforderlichkeit zur Aufgabenerfüllung, bei nicht-öffentlichen Stellen (Abs. 8) auf die Glaubhaftmachung des berechtigten Interesses an der Kenntnis der Daten abgestellt.

Zu den berechtigten Interessen zählt hier jedes von der Rechtsordnung als schutzwürdig anerkannte oder ideelle oder vermögenswerte Interesse des Empfängers der Daten. Dazu gehören auch wirtschaftliche Interessen. Zur Glaubhaftmachung genügt die in sich schlüssige Darstellung des berechtigten Interesses, wobei ergänzend auf Folgendes hinzuweisen ist: Auch wenn die Auskunftsvoraussetzungen des § 14 GewO vorliegen, bedeutet dies nicht zwangsläufig, dass ein Auskunftsanspruch besteht; denn die Gewerberegister sind keine öffentlichen Register. Vielmehr steht die Auskunftserteilung im pflichtgemäßen Ermessen der Behörde.

Hier wird deutlich, dass eine Veröffentlichung der Gewerbemeldungen im Internet den Sinn und Zweck der Regelungen des § 14 GewO grundsätzlich in Frage stellt, da nicht mehr zu kontrollieren wäre, wer auf die Daten zugreift. Das informationelle Selbstbestimmungsrecht der Betroffenen ist hierdurch in einem wesentlich größeren Ausmaß berührt als bei begründeten Auskunftsersuchen gegenüber der Gewerbebehörde. Gegen eine Einstellung in das Internet wären nur dann keine Einwände zu erheben, wenn die Betroffenen vor einer Veröffentlichung ihrer personenbezogenen Daten im Internet ihre (informierte) Einwilligung erteilt hätten. In diesem Zusammenhang wären die Gewerbetreibenden darauf hinzuweisen, dass sich bei der Einspeisung in das Internet Gefahren für die Datensicherheit ergeben. So könnten Unbefugte mit wenig Aufwand Daten verändern oder löschen. Daraufhin wurde auf das Vorhaben verzichtet.

14.3 Bundeseinheitliche Wirtschaftsnummer?

Im 19. Tätigkeitsbericht (Tz. 14.2) hatte der LfD die Erprobung einer bundeseinheitlichen Wirtschaftsnummer dargestellt, die für Unternehmen, Betriebe und sonstige wirtschaftlich Tätige eingeführt werden sollte. Das Gesetz zur Vorbereitung einer bundeseinheitlichen Wirtschaftsnummer bildete die Rechtsgrundlage für die Erprobung.

Der Schlussbericht der Bundesagentur für Arbeit kommt zu dem Ergebnis, dass der isolierten Einführung einer bundeseinheitlichen Wirtschaftsnummer nicht die erwarteten Synergie- und Einsparungseffekte gegenüberstünden. Zwischenzeitlich sei auch mit In-Kraft-Treten des Steueränderungsgesetzes 2003 in § 139 c AO die Voraussetzung für eine einheitliche Wirtschafts-Identifikationsnummer geschaffen worden (vgl. auch Tz. 13.3). Daher wurde empfohlen, zur eindeutigen Identifizierung der Wirtschaftseinheiten gegenüber Verwaltungsstellen die Identifikationsnummer nach deren Einführung zu nutzen.

14.4 Von den Zwecken der Datenübermittlung durch die IHK

Gelegentlich werden Fragen an den LfD herangetragen, die im Zusammenhang mit Datenübermittlungen seitens der Industrie- und Handelskammern stehen.

Die Zulässigkeit und Voraussetzung der Übermittlung von Daten durch die Kammern an nicht-öffentliche Stellen ist in § 9 Abs. 4 IHK-Gesetz geregelt. Hier ist zu unterscheiden zwischen Daten, zu deren Weitergabe die Kammern zur Förderung von Geschäftsabschlüssen sowie zu anderen dem Wirtschaftsverkehr dienenden Zwecken in jedem Fall berechtigt sind, und Daten, die zu diesem Zweck nur dann an nicht-öffentliche Stellen weitergegeben werden dürfen, wenn der Kammerzugehörige nicht widerspricht.

Zur ersten Gruppe gehören der Name, die Anschrift und der Wirtschaftszweig des Kammerzugehörigen. Es handelt sich hierbei um Daten, die aus der Sicht des Betroffenen wohl regelmäßig unsensibel sind, weil er sich mit ihnen zur Verwirklichung seines Geschäftszwecks ohnehin freiwillig in die Öffentlichkeit (z. B. bei der Werbung) begibt; andererseits ist die Weitergabemöglichkeit dieser Daten aus der Sicht der Kammern das Minimum dessen, was sie zur Erfüllung ihres gesetzlichen Auftrags, für die Förderung der gewerblichen Wirtschaft zu wirken (vgl. § 1 Abs. 1 IHK-Gesetz), benötigen und was zur Erreichung des gesetzgeberischen Ziels des § 9 Abs. 4 IHK-Gesetz, Geschäftsabschlüsse zu fördern, notwendig ist. Die Übermittlung weiterer Daten ist nur dann zulässig, wenn der Kammerzugehörige nicht widersprochen hat. Die Kammerzugehörigen sind schriftlich auf die Möglichkeit des Widerspruchs hinzuweisen. Dies geschieht in der Praxis in der Weise, dass der Hinweis bereits in dem ersten Schreiben, das ein neuer Kammerzugehöriger von seiner Kammer erhält, erfolgt. Für den Widerspruch selbst ist keine Form vorgeschrieben.

Sofern die IHK lediglich die „Grunddaten“ (dazu gehören der Name, die Anschrift und der Wirtschaftszweig des Kammerzugehörigen) übermittelt, ist dies nach der Gesetzeslage meist zulässig.

Es gibt jedoch auch Sachverhalte, bei denen die Zweckbestimmung Probleme bereitet. Liegt z. B. im Zusammenhang mit der Einladung zu einer Veranstaltung, bei der es um Fragen der Familien- und Bildungspolitik geht, ein anderer, dem Wirtschaftsverkehr dienender Zweck vor, der nach § 9 Abs. 4 IHK-Gesetz eine Datenübermittlung durch die Kammer erlauben würde? Hier könnte man argumentieren, dass die Familien- und Bildungspolitik durchaus einen Bezug zur und Auswirkungen auf die Wirtschaft haben kann, z. B. bei der Gründung von Betriebskindergärten sowie bei der schulischen und beruflichen Ausbildung. Fraglich ist allerdings, ob eine Übermittlung der Grunddaten auch an außerhalb der Wirtschaft stehende Interessenverbände (Religionsgemeinschaften etc.) nach dem IHK-Gesetz zulässig ist. Angesichts der relativ geringen Schutzwürdigkeit der Grunddaten haben die Kammern hier zwar einen Ermessensspielraum, der sie allerdings nicht von der Verantwortung entbindet, auf die Zulässigkeit der Datenübermittlung – jeweils bezogen auf den konkreten Sachverhalt – zu achten.

14.5 Außenstellen der Kfz-Zulassung in Verbandsgemeindeverwaltungen?

Eine Kreisverwaltung hatte angefragt, ob es zulässig ist, Außenstellen der Kfz-Zulassung in Verbandsgemeindeverwaltungen anzusiedeln. Im Rahmen der Zuständigkeit war darauf hinzuweisen, dass es unter dem Gesichtspunkt des Datenschutzes zunächst nur um die Frage gehen kann, ob hier eine Datenverarbeitung im Auftrag nach den Bestimmungen des Landesdatenschutzgesetzes vorliegt.

Nach Mitteilung der anfragenden Kreisverwaltung sollten Bedienstete einer Verbandsgemeindeverwaltung die Tätigkeit der Kfz-Zulassung voll umfänglich ausüben.

Dies würde die Übertragung hoheitlicher Aufgaben von der Kreisverwaltung auf die Verbandsgemeinde bedeuten. So wäre die Verbandsgemeindeverwaltung im Rahmen des Zulassungsvorgangs für die Aufnahme des Antrags und die Kontrolle der Halterpersonalien, das Bedrucken, die Bestempelung und Aushändigung der Fahrzeugpapiere sowie für die Plakettierung der Kennzeichen und die Kontrolle der Versicherungsbestätigungen zuständig. Dazu wäre es erforderlich, der Verbandsgemeindeverwaltung Blanko-Fahrzeugscheinvordrucke, Dienststempel und Prüfplaketten zu überlassen.

Im Hinblick auf die datenschutzrechtlichen Anforderungen bei der Auslagerung von Datenverarbeitungsaufgaben hat der LfD erläutert, dass das Landesdatenschutzgesetz für öffentliche Stellen die rechtliche Möglichkeit bietet, Datenverarbeitung im Auftrag zu betreiben. Diese Verarbeitungsform liegt vor, wenn die Vereinbarung zwischen den beteiligten Stellen den Voraussetzungen des § 4 LDSG entspricht. Nach Absatz 1 Satz 1 und 2 dieser Bestimmung ist die Auftraggeberin verantwortliche Stelle mit der Folge, dass die Auftragnehmerin, bezogen auf die Aufgabenerledigung, nicht selbst verantwortliche Stelle nach den Vorschriften des LDSG sein kann. Bei der Auftragsdatenverarbeitung im Anwendungsbereich des § 4 LDSG unterstützt die Auftragnehmerin die Auftraggeberin dementsprechend lediglich in einer oder mehreren Phasen der Datenverarbeitung. Nimmt die Auftragnehmerin dagegen mehr als eine „Hilfsfunktion“ wahr, weil ihr neben der einschlägigen Datenverarbeitung für die Auftraggeberin weitere Aufgaben (bzw. Funktionen) zur eigenständigen Erfüllung überantwortet werden, ändert sich der datenschutzrechtliche Charakter der Rechtsbeziehung zwischen den Beteiligten. Dies ist hier der Fall; denn es sollte die zur funktionalen Erledigung der Aufgaben notwendige Sachbearbeitung aus der Kreisverwaltung ausgegliedert und auf eine Verbandsgemeindeverwaltung übertragen werden. Diese Gestaltung lässt sich allerdings nicht mehr unter den Begriff der datenschutzrechtlichen Auftragsdatenverarbeitung einordnen, so dass § 4 LDSG als Rechtsgrundlage ausscheidet.

Allgemein hat der LfD darauf hingewiesen, dass für die beabsichtigte Funktionsübertragung möglicherweise § 7 Verkündungsgesetz zu beachten ist, wonach die Verlagerung von Zuständigkeiten einer gesetzlichen Grundlage bedarf.

14.6 Einführung der Lkw-Maut auf Autobahnen

Bereits im Jahr 2001 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung auf die datenschutzrechtlichen Probleme, die mit der Einführung des Mautsystems verbunden sind, hingewiesen und bei der Mauterfassung eine datensparsame Technik gefordert. Am 1. Januar 2005 wurde nunmehr mit der Erhebung der Lkw-Maut auf Autobahnen begonnen. Die Diskussion über die damit verbundenen Datenschutzfragen – insbesondere bzgl. der Ausweitung des Mautsystems auf andere Fahrzeuge – geht indessen weiter.

Das Autobahnmautgesetz sieht die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen vor und bestimmt ausdrücklich, dass die erhobenen Daten ausschließlich zum Zwecke des Autobahnmautgesetzes verarbeitet und genutzt werden dürfen. Dennoch wurden Begehrlichkeiten wach und vereinzelt Auffassungen vertreten, wonach die nach dem Autobahnmautgesetz erhobenen Daten an Strafverfolgungsbehörden übermittelt werden dürfen. Diesbezüglich hat der Bundesgesetzgeber bei der Novellierung des Autobahnmautgesetzes (BT-Drs.15/3678; BGBl.I S.3121) im Wege einer Konkretisierung der Zweckbindungsregelungen die §§ 4 Abs. 2 und 7 Abs. 2 ABMG um folgenden Satz ergänzt: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig."

14.7 Telefax in Bußgeldangelegenheiten?

Ein Petent fühlte sich in seinen Persönlichkeitsrechten dadurch beeinträchtigt, dass ihm seitens einer Bußgeldstelle als Halter eines Fahrzeugs, das unter seiner Privatadresse zugelassen war, eine schriftliche Verwarnung mit Verwarnungsgeld/Anhörung per Telefax in seine Kanzlei übermittelt wurde, die er mit weiteren Kollegen betreibt.

Hier war auf Folgendes hinzuweisen: Die verantwortliche öffentliche Stelle ist gem. § 9 Abs. 1 LDSG verpflichtet, die zur Einhaltung des Datenschutzes erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zu treffen. Nach § 9 Abs. 2 Nr. 4 LDSG ist insbesondere zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen werden können. Bei der Zustellungsart mittels Telefax besteht die Gefahr, dass Dritte (hier: Berufskollegen und weiteres Personal) ohne weiteres Einblick in den Inhalt des Verwarnungsschreibens mit personenbezogenen Daten erhalten.

Wenn in der Vergangenheit – wie von der Verwaltung dargestellt – bei entsprechenden Briefsendungen an die Privatanschrift des Petenten der Zugang bestritten wurde, hätte eine andere Versandart, beispielsweise die Zustellung per Postzustellungsurkunde, erwogen werden können, um nicht unnötigerweise Dritten den Status des Adressaten als Betroffenen in einem Verwarnungsgeldverfahren zu offenbaren.

Künftig – so wurde dem LfD mitgeteilt – wird die Bußgeldstelle davon Abstand nehmen, persönliche Mitteilungen in Bußgeldangelegenheiten an die Faxadresse des Petenten zu versenden.

Allgemein gehört es zum vertraulichen Umgang mit personenbezogenen Daten, dass Unbefugten der Zugang zu persönlichen Unterlagen verwehrt wird. Öffentliche Stellen müssen bei der (traditionellen) Zustellung von Schriftstücken mit personenbezogenen Daten grundsätzlich verschlossene Briefumschläge verwenden.

14.8 Online-Zugriff des Straßenverkehrsamtes auf den Datenbestand des Passregisters

Zu der seitens einer Stadtverwaltung an den LfD herangetragenen Frage, ob ein Online-Zugriff (automatisiertes Übermittlungsverfahren) des Straßenverkehrsamtes auf den Datenbestand des Passregisters zulässig ist, hat er folgende Auffassung vertreten:

Sofern es nicht möglich ist, die Identität des Fahrzeugführers im Rahmen des Anhörungsverfahrens zu ermitteln, sind weitere Maßnahmen zur Ermittlung der Person, die eine Ordnungswidrigkeit begangen hat, erforderlich und zulässig. In diesen Fällen kann die Verfolgungsbehörde die Pass- und Personalausweisbehörde ersuchen, das Original oder eine geeignete Reproduktion des Personalausweis- bzw. Passfotos des Fahrzeughalters zur Identifizierung vorzulegen oder zu übersenden. Verweigert der Fahrzeughalter die Einlassung zum Sachverhalt oder bestreitet er gefahren zu sein, kann das bei einer Radarüberwachung angefertigte Lichtbild mit dem bei der Ausweisbehörde hinterlegten Lichtbild des Fahrzeughalters abgeglichen werden. Nach § 22 Abs. 2 Passgesetz bzw. nach dem gleichlautenden § 2 b Abs. 2 Personalausweisgesetz ist eine Übermittlung von Pass- bzw. Personalausweisdaten zulässig, wenn die ersuchende Behörde berechtigt ist, solche Daten zu erhalten, sie ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen, und die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss. Diese gesetzlich fixierten Vorgaben bei der Betroffenenermittlung per Lichtbildabgleich können im Rahmen des Einsatzes eines automatisierten Übermittlungsverfahrens (Online-Zugriff) nicht eingehalten werden. Aus den vorgenannten Bestimmungen geht klar und eindeutig hervor, dass ein routinemäßiger Abgleich von Passbildern nicht zulässig ist. Vielmehr hat die Verfolgungsbehörde in jedem Einzelfall zu prüfen, ob die Voraussetzungen dieser Ausnahmevorschriften erfüllt sind. In jedem Fall gilt das Verhältnismäßigkeitsprinzip und der damit verbundene Erforderlichkeitsgrundsatz. Dem wird bei Anwendung der Grundsätze Rechnung getragen, die in einem Rundschreiben des Ministeriums des Innern und für Sport vom 10. Juni 1996, MinBl. 1996, S. 342 (zuletzt geändert durch Rundschreiben vom 26. März 2002, MinBl. 2002, S. 308) für entsprechende Lichtbildanforderungen aus dem Pass- und Personalausweisregister festgelegt sind (vgl. hierzu 19. Tb., Tz. 5.1).

15. Landwirtschaft, Weinbau und Forsten

15.1 Datenübermittlung im Rahmen der Tierseuchenbekämpfung

Eine Kreisverwaltung bat um Überprüfung, ob es aus datenschutzrechtlicher Sicht zulässig sei, Landwirten Anschriften der Betriebsinhaber von Nachbarbetrieben sowie Angaben zum Tierseuchenstatus zu übermitteln. Dadurch sollte den Landwirten ermöglicht werden, ihre BHV1-freien Tiere (BHV = Bovines Herpesvirus) von den Tieren der Nachbarbetriebe, die keinen entsprechenden Impfstatus haben, fernzuhalten, um mögliche Infizierungen zu vermeiden.

Eine Datenübermittlung an nicht-öffentliche Stellen ist unter den Voraussetzungen von § 16 LDSG zulässig. Danach kommt eine Übermittlung u. a. dann in Betracht, wenn die Stelle, der die Daten übermittelt werden, ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen (§ 16 Abs. 1 Nr. 3 LDSG). Ein rechtliches Interesse ist jedes von der Rechtsordnung geschützte Interesse. Ein solches rechtliches Interesse bestand hier nicht. Zwar obliegt es nach dem Tierseuchengesetz i. V. m. der BHV1-Verordnung den Landwirten und Aufsichtsbehörden, tierseuchenfreie Viehbestände zu gewährleisten. Im Falle einer Erkrankung des Tierbestandes drohen dem Halter massive Einschränkungen von der Beschränkung des Viehbetriebs bis hin zur Schlachtung der Tiere. Wenn ihm ein solcher Schaden durch Ansteckung seines Viehbestands beim Nachbarbetrieb entsteht, könnte er gegen diesen u. U. Ersatzansprüche geltend machen. Ein solches Rechtsverhältnis besteht aber zum Zeitpunkt, in dem eine Ansteckung verhindert werden soll, noch nicht. Die Voraussetzungen des § 16 Abs. 1 Nr. 3 LDSG zur Datenübermittlung an nicht-öffentliche Stellen waren daher nicht erfüllt.

Doch war davon auszugehen, dass eine Information sowohl im öffentlichen Interesse als auch im berechtigten Interesse der Tierhalter liegt, so dass eine Datenübermittlung gem. § 16 Abs. 1 Nr. 4 LDSG in Betracht kam. Dies setzte jedoch voraus, dass die Betroffenen nach Unterrichtung über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck der Datenübermittlung nicht widersprochen haben. Da es sich um eine große Anzahl Betroffener handelte, war es nicht unbedingt erforderlich, diese persönlich anzuschreiben. Es wäre auch denkbar gewesen, die Betroffenen über ein geeignetes Veröffentlichungsmedium zu erreichen. Diese waren dabei auf ihr Widerspruchsrecht hinzuweisen. Hierfür konnte die Kreisverwaltung eine angemessene Frist setzen. Diejenigen, denen die Daten übermittelt werden sollten, durften diese nur für den Übermittlungszweck verwenden. Die Datenempfänger waren von der Kreisverwaltung auf diese Zweckbindung hinzuweisen (§ 16 Abs. 4 LDSG).

16. Statistik

16.1 Ämterübergreifende Aufgabenerledigung

Aufgrund einer Empfehlung der Rechnungshöfe des Bundes und der Länder vom November 2002 haben die Statistischen Landesämter und das Statistische Bundesamt ihre bereits bei der Softwareentwicklung praktizierte Zusammenarbeit auf andere statistische Arbeiten ausgedehnt. Um die Effizienz bei der Aufgabenerledigung zu steigern und Kosten zu senken, sollen nach dem Prinzip „Einer für Alle“ einzelne Statistikämter künftig die Statistikaufbereitung für andere Ämter erledigen.

Zunächst war geplant, die Zusammenarbeit in einer Verwaltungsvereinbarung zu regeln. Der Entwurf ging davon aus, dass die Aufbereitungsarbeiten für andere statistische Ämter datenschutzrechtlich als Datenverarbeitung im Auftrag zu charakterisieren seien. So hätte das Statistische Landesamt Rheinland-Pfalz auf der Grundlage des § 6 LStatG z. B. die zu erledigenden Aufgaben im Bereich des Bevölkerungsstatistikgesetzes an ein anderes Statistisches Landesamt vergeben können. Die landesrechtlichen Vorschriften in anderen Bundesländern führten jedoch zu rechtlichen Hindernissen, die das geplante Vorgehen nicht erlaubten. Hier war eine einheitliche gesetzliche Regelung der ämterübergreifenden Aufgabenerledigung erforderlich, die zwischenzeitlich durch eine entsprechende Änderung des Bundesstatistikgesetzes auch vorliegt (vgl. Art. 2 des Gesetzes zur Änderung des Statistikregistergesetzes und sonstiger Statistikgesetze vom 9. Juni 2005, BGBl. I S. 1534). Mit der Einfügung eines § 3 a BStatG wurde die rechtliche Grundlage für eine neue Arbeitsteilung nach dem Prinzip „Einer oder Einige für Alle“ zwischen den statistischen Ämtern des Bundes und der Länder geschaffen. Die Zusammenarbeit bezieht sich auf die Durchführung von Bundesstatistiken und sonstigen Arbeiten statistischer Art im Rahmen der Bundesstatistik. Zu den sonstigen Arbeiten statistischer Art gehört z. B. die Führung des Unternehmensregisters nach dem Statistikregistergesetz.

Des Weiteren stellt eine Ergänzung in § 16 Abs. 2 BStatG klar, dass im Rahmen einer Zusammenarbeit der statistischen Ämter nach § 3 a BStatG auch die Übermittlung von Einzeldaten zwischen statistischen Ämtern sowie deren Verarbeitung und Nutzung in einem oder mehreren Ämtern für andere Ämter zulässig ist.

16.2 Aufbau eines Forschungsdatenzentrums der Statistischen Landesämter

Durch die Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik wurden im Auftrag des Bundesministeriums für Bildung und Forschung verschiedene Vorschläge zur Verbesserung der Wechselwirkungen zwischen Wissenschaft und Statistik erarbeitet. Eine der zentralen institutionellen Empfehlungen dieser Kommission bestand in der möglichst raschen Einrichtung von Forschungsdatenzentren bei den öffentlichen Datenproduzenten. Das Statistische Bundesamt hat daraufhin für seinen Zuständigkeitsbereich ein derartiges Forschungszentrum gegründet. Etwa 90 Prozent der Daten, aus denen

Bundesstatistiken erstellt werden, befinden sich allerdings im Verfügungsbereich der Statistischen Landesämter. Diese haben dementsprechend ebenfalls ein Forschungsdatenzentrum gegründet, das von einem Lenkungsausschuss geleitet wird. Mit den beiden Forschungsdatenzentren intensiviert die deutsche amtliche Statistik ihre Bemühungen, Mikrodaten der amtlichen Statistik für wissenschaftliche Analysen zugänglich zu machen.

Über das Datenschutzkonzept für das Forschungsdatenzentrum der Statistischen Landesämter wurde zwischen den Statistischen Landesämtern und den Landesdatenschutzbeauftragten diskutiert. Dabei ging es insbesondere um Fragen der rechtlichen Grundlagen einer Zentralisierung der Statistiken bei einzelnen Landesämtern (vgl. hierzu Tz. 16.1) und die Form des Bereitstellens von Mikrodaten für die Wissenschaft. In diesem Zusammenhang hat der LfD gegenüber dem Präsidenten des Statistischen Landesamtes zum Ausdruck gebracht, dass er das Projekt eines Forschungsdatenzentrums angesichts seiner Notwendigkeit für die Wissenschaft ausdrücklich begrüßt, verbunden mit dem Hinweis, dass die Einrichtung im Echtbetrieb einer noch zu schaffenden Rechtsgrundlage im Bundesstatistikgesetz bedarf. Denn es handelt sich um eine umfassende Änderung der Infrastruktur der amtlichen Statistik, die dauerhaft etabliert werden soll. Um das Projekt in der Testphase nicht zu blockieren und einen aussagefähigen Testbetrieb zu gewährleisten, wurde in den Grundzügen erörtert, welche Maßnahmen aus der Sicht des Datenschutzes erforderlich sind. Für den regionalen Standort Bad Ems (Sitz des Statistischen Landesamtes) wurde ein IT-Sicherheitskonzept vorgelegt, das insbesondere die organisatorischen Bedingungen und die technische Infrastruktur beschreibt. In seiner Endfassung ist die Nutzung durch die Wissenschaft auf faktisch anonymisierte Mikrodaten beschränkt worden.

Der Bundesgesetzgeber hat die Notwendigkeit einer gesetzlichen Regelung für den Echtbetrieb der Forschungsdatenzentren erkannt und inzwischen entsprechende rechtliche Grundlagen geschaffen. Im Zuge einer Änderung des Bundesstatistikgesetzes (vgl. hierzu Tz. 16.1) stellt § 3 a Abs. 2 BStatG klar, dass die statistischen Ämter auch bei der Bereitstellung von Daten für die Wissenschaft zusammenarbeiten können. Wie sich aus der Entwurfsbegründung (vgl. BT-Drs. 15/4955 zu Art. 2, Nr. 1 vom 23. Februar 2005) ergibt, „zählen zur Wissenschaft vor allem die in § 16 Abs. 6 BStatG genannten Hochschulen und sonstigen Einrichtungen, die mit der Aufgabe unabhängiger wissenschaftlicher Forschung betraut sind. Eine solche Bereitstellung umfasst neben der Veröffentlichung von aggregierten Daten als klassischer Form der Verbreitung statistischer Ergebnisse auch die Nutzbarmachung statistischer Daten, z. B. in Forschungsdatenzentren, in Form von anonymisierten Mikrodaten (Public und Scientific Use Files) oder auf andere geeignete Weise.“ Aus einer Änderung in § 16 Abs. 2 BStatG ergibt sich gemäß der Entwurfsbegründung ferner, „dass im Rahmen einer Zusammenarbeit der statistischen Ämter nach § 3 a BStatG auch die Übermittlung von Einzeldaten zwischen statistischen Ämtern sowie deren Verarbeitung und Nutzung in einem oder mehreren Ämtern für andere Ämter zulässig ist. Damit wird auch die Zulässigkeit des Betriebs der Forschungsdatenzentren der statistischen Ämter des Bundes und der Länder rechtlich klargestellt.“

Die diesbezüglichen Darlegungen des Statistischen Landesamtes zu den Möglichkeiten der Datennutzung sind in der Anlage 18 zusammenfassend wiedergegeben.

16.3 Neues vom Mikrozensus

Diese repräsentative Haushaltsbefragung der amtlichen Statistik führte, wie in jedem Berichtszeitraum, zu zahlreichen Anfragen der Betroffenen.

Der Mikrozensus ist eine jährliche Befragung von einem Prozent der Haushalte. Um die Aktualität der Ergebnisermittlung zu verbessern, wird sie von 2005 an nicht mehr nur auf einen Stichtag im April beschränkt. Die Erhebung findet vielmehr durch gleichmäßige Verteilung über alle Kalenderwochen des Jahres hinweg statt. Fragebögen gibt es von 2005 an nur noch für Selbstausfüller.

Als zentrales Erhebungsinstrument der Interviewer kommen nunmehr flächendeckend sog. „Tablet-PC“ zum Einsatz. Diese Geräte – ein Exemplar wurde dem LfD anlässlich einer Veranstaltung im Statistischen Landesamt zu Testzwecken zur Verfügung gestellt – ermöglichen die Anwendung komplexer Software. Die verwendeten Computerprogramme schließen durch eine entsprechende Filterführung für bestimmte Personen nicht zutreffende Fragen von vornherein aus und ermöglichen unmittelbare Plausibilitätskontrollen. Bei unstimmigen Antworten können die Interviewer direkt nachfragen und eventuelle Missverständnisse aus dem Weg räumen.

Jeder Umgang öffentlicher Stellen mit personenbezogenen Daten, also auch das Erheben und Speichern solcher Daten bei der Durchführung des Mikrozensus, bedarf als Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage. Die rechtlichen Voraussetzungen für die Übernahme des neuen Konzepts zur Erhebung 2005 wurden mit dem Mikrozensusgesetz vom 24. Juni 2004 (BGBl. I S. 1350) geschaffen.

Dabei handelt es sich um die folgenden Mikrozensus-Erhebungsmerkmale für die Jahre 2005 bis 2012:

Jährlich erhoben werden Merkmale der Person bzgl. Familien- und Haushaltszusammenhang, Lebensgemeinschaft, Staatsangehörigkeit, Haupt- und Nebenwohnung, Quellen des Lebensunterhalts, Höhe des Einkommens, Rentenversicherung, allgemeine und berufliche Ausbildung, Schule, Hochschule, Erwerbstätigkeit, Arbeitslosigkeit und Arbeitssuche.

Merkmale, die im Abstand von vier Jahren erhoben werden, sind

- in den Jahren 2005 und 2009 die Lebensversicherung, Schichtarbeit und betriebliche Altersversorgung, Gesundheit und Behinderung sowie Staatsangehörigkeit der Eltern,
- in den Jahren 2006 und 2010 die Wohnsituation,
- in den Jahren 2007 und 2011 die Krankenversicherung sowie ausgeübte Tätigkeit und Stellung im Betrieb,
- in den Jahren 2008 und 2012 die Pendlereigenschaft.

Eine weitere Neuerung enthält das Mikrozensusgesetz 2005 in § 13, wonach das Bundesministerium des Innern ermächtigt wird, mit Zustimmung des Bundesrates Verordnungen zur Änderung des Katalogs der Erhebungsmerkmale zu erlassen.

Für die vom Mikrozensus betroffenen Personen besteht grundsätzlich eine gesetzliche Auskunftspflicht. Sie sind verpflichtet, bei der Erhebung die gestellten Fragen wahrheitsgemäß und vollständig zu beantworten. Persönliche Befreiungsgründe sieht das Gesetz nicht vor. Eine Verletzung der Auskunftspflicht stellt zwar keine Ordnungswidrigkeit dar; doch kann bei Auskunftsverweigerung nach den Regelungen des Verwaltungsvollstreckungsgesetzes ein Zwangsgeld angedroht und festgesetzt werden.

Einige Auskünfte sind freiwillig. Darunter fallen neben der Mitteilung der Telekommunikationsnummer u. a. die Angaben zu Wohn- und Lebensgemeinschaften, zum Bestehen und zur Höhe einer Lebensversicherung sowie zum Gesundheitszustand. Freiwillig sind auch die Angaben ausländischer Personen zu den im Ausland lebenden Kindern, Ehepartnern oder Eltern.

Die Interviewerinnen und Interviewer, deren Besuch zuvor schriftlich angekündigt wird, sind Erhebungsbeauftragte des Statistischen Landesamtes und eigens mit der Mikrozensusbefragung betraut. Die Erhebungsbeauftragten sind, wie alle Mitarbeiterinnen und Mitarbeiter des Landesamtes, zur Geheimhaltung verpflichtet. Um dennoch Interessenkonflikte zu vermeiden, dürfen z. B. keine Personen aus der unmittelbaren Nachbarschaft als Erhebungsbeauftragte eingesetzt werden.

17. Personaldatenschutz

17.1 Telearbeit

Bereits im 17. Tb. (Tz. 17.3) hatte der LfD zu den rechtlichen Rahmenbedingungen, die aus datenschutzrechtlicher Sicht bei der Einrichtung von Telearbeitsplätzen zu beachten sind, Stellung genommen. Er vertrat dabei die Auffassung, dass Tele- bzw. Heimarbeit bei der Verarbeitung von personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, grundsätzlich nicht in Betracht kommt.

Im Berichtszeitraum wurden an den LfD Anfragen herangetragen, in denen gerade die Verarbeitung dieser besonders sensiblen Daten am Heimarbeitsplatz in Rede stand. Eine Krankenkasse hatte vor, Sozialdaten am Heimarbeitsplatz verarbeiten zu lassen, die OFD plante Ähnliches mit Steuerdaten und im Bereich der Schulaufsicht ging es um das Vorhalten von Personaldaten am Heimarbeitsplatz.

Der LfD wies darauf hin, dass die betroffenen Personen, deren Daten im Wege der Telearbeit verarbeitet werden, einen Anspruch darauf haben, dass ihre Daten am Heimarbeitsplatz einem vergleichbaren Schutzniveau unterliegen, wie dies bei einer Verarbeitung in der Dienststelle der Fall wäre. Dem sind jedoch rechtliche Grenzen gesetzt:

- Im Gegensatz zu den Kontrollbefugnissen gegenüber öffentlichen Stellen des Landes stehen den Mitarbeitern des LfD wegen der Unverletzlichkeit der Wohnung (Art. 13 GG) keine gesetzlichen Betretungsrechte für Kontrollzwecke am Heimarbeitsplatz zu. Wenn also der Telearbeiter oder ein Mitbewohner den Zutritt verweigert, kann die Kontrolle nicht durchgeführt werden.
- Weiterhin besteht sowohl auf dem Übermittlungsweg als auch am Heimarbeitsplatz selbst ein erhöhtes Risiko, dass Unbefugte Kenntnis von sensiblen Informationen erhalten.
- Schließlich bestehen am Heimarbeitsplatz geringere Einflussmöglichkeiten des Dienstherrn/behördlichen Datenschutzbeauftragten im Hinblick auf eine ordnungsgemäße Datenverarbeitung.

Aus diesen Gründen hält der LfD an seiner bislang vertretenen restriktiven Auffassung fest. Dies bedeutet: Telearbeit im besonders sensiblen Bereich sollte nicht die Regel sein; Ausnahmen sind jedoch in zu begründenden Einzelfällen möglich. Dabei müssen aus Sicht des LfD folgende Voraussetzungen erfüllt werden:

1. Eine anonymisierte oder pseudonymisierte Datenverarbeitung am Telearbeitsplatz ist nicht möglich,
2. die betroffenen Mitarbeiter können auch nicht anderweitig mit der Verarbeitung weniger sensibler Daten beschäftigt werden,
3. den technisch-organisatorischen Anforderungen wird in besonderem Maße Rechnung getragen (s. Orientierungshilfe „Telearbeit“, abrufbar über das Internetangebot des LfD),
4. die Behördenleitung hat den Ausnahmefall genehmigt,

5. auf der Basis einer Individualvereinbarung werden Zutrittsrechte des behördlichen Datenschutzbeauftragten sowie der Mitarbeiter des LfD vertraglich vereinbart mit der Klausel, dass im Fall des Widerrufs oder einer Zutrittsverweigerung die Telearbeit – soweit personenbezogene Daten betroffen sind – mit sofortiger Wirkung beendet ist und
6. der behördliche Datenschutzbeauftragte sowie der Personalrat sind ordnungsgemäß beteiligt worden.

Im Rahmen der Kontrolltätigkeit des LfD hat sich gezeigt, dass die Telearbeitseignung anhand einer Arbeitsplatzbeschreibung und der konkreten Verhältnisse vor Ort für jeden Fall gesondert zu prüfen ist. So konnte bei der Krankenkasse in der Mehrzahl der Fälle auf die Verarbeitung von personenbezogenen Sozialdaten am Heimarbeitsplatz gänzlich verzichtet werden. Ist dies nicht möglich, sollte eine ausschließlich automatisierte Datenverarbeitung angestrebt werden. Denn bei einer ordnungsgemäßen Absicherung des Rechners ist die Gefahr, dass Unbefugte (z. B. Familienangehörige, Besucher) durch das Herumliegen von Akten Kenntnis von geschützten Daten erhalten, deutlich reduziert.

Die anfragenden Stellen haben die o. g. Vorgaben in Dienstanweisungen, Dienst- und Individualvereinbarungen in datenschutzgerechter Weise umgesetzt. Die Kontrolle einzelner Heimarbeitsplätze durch den LfD wird gleichwohl auch in der Zukunft fortgeführt werden.

17.2 Personaldatenschutz bei der Inruhestandsversetzung von Lehrkräften

Ein ehemaliger Lehrer trug in seiner Eingabe beim LfD Folgendes vor: Er sei wegen Dienstunfähigkeit in den vorzeitigen Ruhestand versetzt worden. In seinem Auftrag habe seine ebenfalls bei der Schule beschäftigte Ehefrau ein Schreiben der ADD entgegengenommen. Das Kuvert sei geöffnet gewesen und habe die Urkunde sowie ein Begleitschreiben enthalten. In diesem Begleitschreiben werde er darauf hingewiesen, dass er verpflichtet sei, alle erforderlichen Behandlungsmaßnahmen zur Verbesserung bzw. Wiederherstellung seiner Dienstfähigkeit „als da wären eine ambulante neuropsychologische Behandlung mit Heimtraining sowie eine Abklärung des fraglichen Alkoholabusus“ durchzuführen.

Der Petent war der Auffassung, dass der an ihn adressierte Brief nicht von der Schulleitung hätte geöffnet werden dürfen. Die Schulleitung habe ihm gegenüber jedoch mitgeteilt, dass der Brief mit einem Beiblatt an die Schule adressiert gewesen sei.

Wiederholte Nachfragen bei der ADD ergaben, dass eine Ablichtung der Ruhestandsversetzung bis dato regelmäßig an die Schulleitung und die OFD übersandt wurde. Diese Praxis war zumindest dann datenschutzrechtlich problematisch, wenn die Verfügung – so wie im vorliegenden Fall – weitergehende Informationen, insbesondere für den Betroffenen belastende Auflagen, enthält. Da ausschließlich die ADD als personalaktenführende Stelle zur Überwachung der Auflagen zuständig ist, war nicht ersichtlich, inwiefern es für die Aufgabenerfüllung der Schulleitung und der OFD erforderlich sein sollte, hiervon in Kenntnis gesetzt zu werden.

Die ADD änderte daraufhin den Standardtext der entsprechenden Verfügung dergestalt ab, dass dem Erforderlichkeitsgrundsatz bei der Übermittlung von Personaldaten künftig Rechnung getragen werden wird.

17.3 Datenverarbeitung bei der Berechnung von Versorgungsbezügen

Im Zusammenhang mit der Festsetzung von Versorgungsbezügen wandte sich ein Petent mit folgendem Sachverhalt an den LfD:

Der Petent bat als künftiger Versorgungsempfänger um informatorische Festsetzung der für ihn zu erwartenden Versorgungsbezüge. Die zuständige Behörde stellte nach Beiziehung der Personalakte u. a. fest, dass sich der Petent in früheren Jahren zu Studienzwecken in den USA aufgehalten hatte. Zur Klärung, ob er im Rahmen dieses Auslandsaufenthaltes möglicherweise einen realisierbaren Rentenanspruch erworben hatte, wandte sich die Behörde schriftlich an das Generalkonsulat der USA. Darin teilte sie u. a. mit, dass im Rahmen der Festsetzung der Versorgungsbezüge des Petenten festgestellt worden sei, dass dieser „auch in den USA einer Beschäftigung nachgegangen“ sei, die möglicherweise nach dortigem Recht zu einem Rentenanspruch geführt haben könnte. In einer tabellarischen Zusammenstellung wurden sodann unter den Überschriften „Auslandstätigkeit“, „Beschäftigungsart“, „Beschäftigungsstelle“ und „Beschäftigungsort“ weitere Angaben zu dem damaligen Aufenthalt gemacht. Das Generalkonsulat wurde schließlich um Prüfung gebeten, ob der Petent einen realisierbaren Rentenanspruch erworben habe und wo dieser ggf. beantragt werden müsse. Sofern datenschutzrechtliche Gründe einer direkten Auskunftserteilung entgegenstehen sollten, wurde um direkte Übersendung der Information an den Petenten und gleichzeitige behördliche Unterrichtung gebeten. Der Petent erhielt eine Abschrift dieses Schreibens.

Tatsächlich war der Petent während seines Studienaufenthaltes in den USA keiner Beschäftigung nachgegangen. Dies teilte er der Behörde unmittelbar nach Erhalt des Schreibens auch mit. In einer ihm gegenüber abgegebenen Stellungnahme rechtfertigte diese unter Hinweis, dass es bei Studienzeiten im Ausland üblich sei, „dass Beamte neben der Ausbildung weitere berufliche Tätigkeiten ausüben, die grundsätzlich auch zu Rentenansprüchen führen können“, eine direkte Befragung des Generalkonsulates. Zudem wurde mitgeteilt, dass in Ansehung der für die Weitergabe der betroffenen Daten an das Generalkonsulat relevanten Vorschriften zum Schutze von Sozialdaten nach dem SGB X, insbesondere von § 69 SGB X, im konkreten Falle ein Verstoß gegen datenschutzrechtliche Bestimmungen nicht gegeben sei.

Gegen die dargelegte Verfahrensweise hatte der LfD erhebliche Bedenken.

Die Zulässigkeit der Verarbeitung von personenbezogenen Daten zur Festsetzung von Versorgungsbezügen eines Beamten beurteilt sich nicht nach den Regelungen des SGB X, sondern nach Beamtenrecht bzw. den allgemeinen Bestimmungen des LDSG. Soweit bei der Berechnung und Festsetzung der Versorgungsbezüge im Hinblick auf die in § 55 Abs. 8 BeamtVG enthaltene Regelung geklärt werden muss, ob der Versorgungsempfänger zugleich gegenüber einem ausländischen Rentenversicherungsträger einen Rentenversicherungsanspruch erworben hat, ist der in § 12 Abs. 2 Satz 1 LDSG enthaltene Direkterhebungsgrundsatz zu beachten. Dies bedeutet, dass zunächst der Betroffene zu den für die Sachverhaltsaufklärung relevanten Tatsachen – frühere Beschäftigung im Ausland, daraus resultierender Erwerb eines Rentenversicherungsanspruches – persönlich befragt werden muss. Denn es ist regelmäßig davon auszugehen, dass der Betroffene zumindest die Frage, ob er überhaupt in der Vergangenheit im Ausland einer Beschäftigung nachgegangen ist, auch beantworten kann. In dem der Eingabe zugrunde liegenden Fall waren zudem keine Anhaltspunkte ersichtlich, die eine Datenerhebung bei Dritten auf der Grundlage des § 12 Abs. 4 LDSG rechtfertigen würden. Insbesondere lagen die Voraussetzungen des § 12 Abs. 4 Nr. 6 LDSG nicht vor, da aus der Personalakte des Petenten nicht zu entnehmen war, dass dieser im Rahmen seines damaligen Studienaufenthaltes überhaupt einer Beschäftigung nachgegangen war und daher auch nicht davon ausgegangen werden konnte, dass er einer entsprechenden Nachfrage bei dem Generalkonsulat bei Kenntnis des Zwecks der Erhebung zugestimmt hätte.

Zudem teilte im Zusammenhang mit der Berechnung der Versorgungsbezüge des Petenten die Behörde dem US-Generalkonsulat unzutreffenderweise mit, es sei festgestellt worden, dass der Petent im Rahmen eines früheren Studienaufenthaltes einer Beschäftigung in den USA nachgegangen sei. Da sich weder aus der Personalakte noch aus sonstigen Unterlagen Hinweise für diese Behauptung ergaben, konnte man von einer früheren Beschäftigung des Petenten in den USA nicht ausgehen, zumal ihm aufgrund des damals erteilten Visums die Aufnahme einer Beschäftigung ausdrücklich untersagt war. Die gleichwohl erfolgte Weitergabe dieser unzutreffenden Information an das Generalkonsulat war somit datenschutzrechtlich unzulässig.

Die betroffene Behörde teilte die rechtliche Bewertung des LfD und passte das zugrunde liegende Verfahren an die datenschutzrechtlichen Vorgaben an.

17.4 GPS-Ausstattung der Fahrzeuge beim Landesbetrieb Straßen und Verkehr

Im Bereich des Landesbetriebs Straßen und Verkehr bestehen Bestrebungen, den analogen Funk durch den digitalen Betriebsfunk zu ersetzen. Hintergrund sind Vereinbarungen des Landesbetriebs mit dem Bundesverkehrsministerium, wonach Rheinland-Pfalz in einem Pilotprojekt als erstes Bundesland die Erneuerung des Betriebsfunks an Bundesautobahnen in digitaler Technik durchführen soll. Mit dem Umstieg auf die Digitaltechnik können neben der Sprache auch Daten übertragen werden. Dies kann man sich beispielsweise im Rahmen eines sogenannten Flottenmanagements zu Nutze machen, bei dem die einzelnen Fahrzeuge mit einem GPS-Sender ausgestattet und die übertragenen Daten auf einem Bildschirm in der Autobahnmeisterei dargestellt werden. Der Einsatzleiter kann sich mit einem Blick auf den Monitor schnell einen Überblick über den Standort der sich im Einsatz befindlichen Fahrzeuge verschaffen und dadurch die Disposition des Betriebsdiensteinsatzes optimieren.

Im Berichtszeitraum wurde die Einführung eines solchen Flottenmanagements in einer mehrwöchigen Testphase erprobt. Wegen der dieser Technik immanenten Überwachungsmöglichkeiten verfolgten die Beschäftigten diese Entwicklung überaus skeptisch und wandten sich an den LfD.

Dieser prüfte die sich im Einsatz befindliche Software und stellte dabei fest, dass neben der geographischen Position der Fahrzeuge (bis zu 20 Meter in der Realität) auch die Funknummer, Kennzeichen, Fahrzeuggeschwindigkeit und -richtung sowie Datum und Uhrzeit auf dem Bildschirm in der Autobahnmeisterei abgebildet wurden. Darüber hinaus war es möglich, bestimmte Auswertungen vorzunehmen. So konnte man sich die zurückgelegte Fahrstrecke eines Fahrzeugs anzeigen lassen oder sich darüber informieren, welches Fahrzeug sich um eine konkrete Uhrzeit an welcher Position befunden hat. Stand- und Fahrzeiten, gefahrene Geschwindigkeiten und die jeweilige Uhrzeit konnten in einem Diagramm dargestellt werden (elektronische Tachoscheibe). Der Auswertungszeitraum betrug – entsprechend der im Testbetrieb vereinbarten Speicherfrist – drei Tage.

Von Seiten der Personalvertretung wurden grundsätzliche Bedenken zur Erforderlichkeit und Verhältnismäßigkeit dieser Form der Mitarbeiterkontrolle angeführt: Eine ausreichende Dokumentation der jeweiligen Einsätze erfolge bereits jetzt über die Tagesberichte, Fahrtenbücher und Tachoscheiben. Der jeweilige Standort der Fahrzeuge würde im Rahmen der täglich stattfindenden Dienstbesprechungen festgelegt und könne bei Bedarf über Funk jederzeit erfragt werden. Ein Bedürfnis, mehrere Fahrzeuge unter Zuhilfenahme des Flottenmanagement-Systems zu koordinieren, bestünde allenfalls im Winterdienst oder bei besonderen Aufgaben, wie etwa der Einrichtung einer Baustelle. Würden die erfassten Daten längere Zeit gespeichert, würde dies in haftungsrechtlichen Fragen zu einer unverhältnismäßigen Risikoverlagerung auf Seiten der Beschäftigten führen.

Von Seiten der Dienststelle wurde andererseits durchaus nachvollziehbar dargelegt, dass aufgrund der Größe des Zuständigkeitsbereiches, der Anzahl der Einsatzfahrzeuge sowie der Anzahl der bei der Autobahnmeisterei beschäftigten Mitarbeiter die Koordination und Disposition der Fahrzeuge durch den Einsatz von GPS-gestützter Technik erheblich erleichtert werden könne.

Im Hinblick darauf, dass es sich bei der Einführung der o. g. Software um eine mitbestimmungspflichtige Maßnahme nach § 80 Abs. 2 Ziff. 2 und 3 LPersVG handelte, empfahl der LfD, im Rahmen einer Dienstvereinbarung u. a. folgende Punkte festzulegen:

- Regelung, wann das GPS-gestützte Flottenmanagementverfahren zum Einsatz kommen soll (routinemäßig oder nur ereignisabhängig, wenn dies etwa aufgrund der Wetterlage oder aufgrund einer besonderen Aufgabenstellung erforderlich ist);
- Regelung, welche Fahrzeuge eine GPS-Ausstattung erhalten;
- Schaffung von Möglichkeiten zur Kenntlichmachung der Überwachung (Beispiel: bedarfsweise Aktivierung durch die Fahrzeugbesatzung mittels Schalter);
- Dauer der Speicherung;
- Festlegung der Zugriffs- und Auswertungsbefugnisse;
- Regelung, wonach disziplinarische oder arbeitsrechtliche Maßnahmen nicht ausschließlich auf das GPS-gestützte Flottenmanagementverfahren gestützt werden dürfen, Verbot allgemeiner Verhaltens- und Leistungskontrollen;
- Übertragung nur der tatsächlich erforderlichen Fahrzeugdaten;
- Protokollierung der Auswertungen bzw. des Heranzoomens ab einer bestimmten Zoom-Stufe.

Der Personalrat konnte beim Abschluss der Dienstvereinbarung die datenschutzrechtlichen Interessen der Mitarbeiter weitgehend durchsetzen.

17.5 Kühe im Rampenlicht

Ein nicht ganz alltäglicher Sachverhalt beschäftigte den LfD im Rahmen einer an ihn gerichteten behördlichen Anfrage einer Lehr- und Versuchsanstalt für Viehhaltung. Dort beabsichtigte man den mit Milchkühen besetzten Liegeboxenlaufstall während eines fünfmonatigen Versuchs mit Videokameras zu beobachten. Mit dem Versuch sollte über den gesamten Tagesablauf das Verhalten der Tiere im Hinblick auf die unterschiedlichen in den Liegeboxen verlegten Beläge sowie der sich daraus jeweils ergebende Betreuungs- bzw. Arbeitszeitbedarf ermittelt werden. Die datenschutzrechtliche Relevanz der Angelegenheit lag darin, dass von der Dauerbeobachtung auch die in diesem Bereich tätigen Mitarbeiter der Lehr- und Versuchsanstalt betroffen waren, von denen einer trotz der bereits erteilten Zustimmung des Personalrates Bedenken äußerte. Eine Rückfrage ergab, dass die Mitarbeiter täglich durchschnittlich 20 Minuten lang beobachtet werden sollten.

Im Ergebnis hatte der LfD gegen die beabsichtigte Versuchsdurchführung keine Einwände. Ausgehend von der Annahme, dass bei den in diesem Bereich eingesetzten Mitarbeitern die Durchführung oder Unterstützung von Versuchen, die der Aufgabenerfüllung der Lehr- und Versuchsanstalt dienen, ohnehin zu der arbeitsvertraglich zu erbringenden Leistung gehört, wäre eine in diesem Zusammenhang erforderliche Verarbeitung von Beschäftigtendaten auf der Grundlage des § 31 Abs. 1 Satz 1 LDSG datenschutzrechtlich zulässig, zumal die Beobachtungsdauer bezogen auf die tägliche Arbeitszeit sehr gering war und eine ordnungsgemäße Beteiligung der Personalvertretung erfolgt war. Der anfragenden Stelle wurde empfohlen, im Rahmen einer Dienstvereinbarung den Verwendungszweck, den Kreis der Zugriffsberechtigten sowie die Speicherdauer festzulegen. Inhaltlich sollte dabei u. a. eine Nutzung der Aufzeichnungen zur Durchführung von Verhaltens- und Leistungskontrollen der Betroffenen ausdrücklich ausgeschlossen und eine Löschung der personenbezogenen Aufnahmen nach Abschluss der Versuchsauswertung sichergestellt werden.

18. Datenschutz im kommunalen Bereich

18.1 Briefzustellung durch private Dritte

Aus verschiedenen Gründen übertragen immer mehr öffentliche Stellen die Zustellung ihrer Briefpost privaten Unternehmen. So wurde der LfD im Berichtszeitraum beispielsweise von einer Kreisverwaltung um Bewertung eines derartigen Vorhabens gebeten. Dies war deshalb von besonderer Bedeutung, da von der beabsichtigten Maßnahme sämtliche Bereiche der Kreisverwaltung und somit auch solche Daten betroffen waren, die z. B. als Gesundheits- oder Sozialdaten besonderen Berufs- oder Amtsgeheimnissen unterworfen sind.

Datenschutzrechtlich stellt die Übertragung der Briefzustellung auf einen privaten Dritten eine Verarbeitung personenbezogener Daten im Auftrag dar, die den generellen Anforderungen des § 4 LDSG unterliegt. Besonders hinzuweisen ist in diesem Zusammenhang auf die Regelung des § 4 Abs. 1 Satz 3 LDSG, wonach sich der Auftragnehmer, sollte er keine öffentliche Stelle des Landes Rheinland-Pfalz i. S. d. § 2 Abs. 1 LDSG sein, der Kontrolle des Landesbeauftragten für den Datenschutz zu unterwerfen hat. Soweit darüber hinaus nach § 4 Abs. 4 Satz 2 LDSG eine Auftragsvergabe an nicht-öffentliche Stellen nur dann zulässig ist, wenn überwiegende schutzwürdige Interessen, insbesondere Berufs- oder besondere Amtsgeheimnisse, nicht entgegenstehen, ist zu beachten, dass der Auftragsgegenstand – die regelmäßige Beförderung von Briefsendungen – eine Postdienstleistung i. S. v. § 4 Abs. 1 a PostG darstellt und nach § 39 Abs. 2 PostG derjenige, der geschäftsmäßig Postdienste erbringt oder daran mitwirkt, zur Wahrung des Postgeheimnisses verpflichtet ist. Weiterhin gelten für diese Unternehmen die bereichsspezifischen datenschutzrechtlichen Vorgaben des § 41 PostG bzw. der hierzu erlassenen Postdienste-Datenschutzverordnung. Sofern der in Frage kommende Auftragnehmer den Anforderungen des Postgesetzes zur Lizenzierung (§§ 5 ff. PostG) entspricht, stehen überwiegende schutzwürdige Interessen der Betroffenen einer Auftragsvergabe nicht entgegen.

18.2 Einsatz privater Sicherheitsdienste durch kommunale Ordnungsämter

Der Einsatz privater Sicherheitsdienste durch kommunale Ordnungsämter in Rheinland-Pfalz befindet sich seit Ende 2004 in der öffentlichen Diskussion. Das Thema war u. a. Gegenstand einer Kleinen Anfrage im Landtag Rheinland-Pfalz, die mit Schreiben vom 1. Oktober 2004 durch die Landesregierung beantwortet wurde (vgl. LT-Drs. 14/3458). Darin bekräftigte das zuständige ISM u. a., dass aufgrund des staatlichen Gewaltmonopols die hoheitlichen Aufgaben der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung nicht auf private Sicherheitsdienste übertragen werden können.

Dem LfD wurden diverse Vorhaben im Lande bekannt. So richtete eine Stadtverwaltung ab Dezember 2004 regelmäßige Streifengänge durch einen privaten Sicherheitsdienst ein. Die Wachpersonen sollten nach den zugrunde liegenden Vereinbarungen u. a. Präsenz zeigen, Ansprechpartner für Bürger und Touristen sein, generell Gefahren und Störungen der öffentlichen Sicherheit und Ordnung an die zuständigen Sicherheitsbehörden melden sowie das Ordnungsamt zeitnah über besondere Vorkommnisse unterrichten. Darüber hinaus wurde ausdrücklich geregelt, dass den Wachpersonen keine Eingriffsbefugnisse zustehen und sie im Wesentlichen Hilfe anbieten und Störer der öffentlichen Sicherheit und Ordnung durch geeignete deeskalierende Ansprache auf ihr Fehlverhalten hinweisen sollen. Der Auftragnehmer hatte aufgrund der vertraglichen Dokumentations- und Mitteilungspflichten sämtliche im Rahmen seiner Tätigkeit festgestellten Auffälligkeiten an den Auftraggeber weiterzugeben. Dies umfasste zwangsläufig auch die Übermittlung der dabei zur Kenntnis genommenen personenbezogenen Informationen. Im Dienstleistungsvertrag war daher eine Passage zum Datenschutz enthalten, in der sowohl eine Nutzung personenbezogener Daten durch den Auftragnehmer als auch eine Weitergabe der Daten durch diesen an Unbefugte untersagt wurde.

Unvermittelt wurde das Vorhaben – wie ein ähnliches bereits zuvor – nach drei Monaten Laufzeit Ende Februar 2005 abgebrochen. Presseberichten war zu entnehmen, dass die mit dem Vorhaben verbundenen Erwartungen nicht erfüllt wurden – die „City-Scouts“ seien schlicht und einfach in der Öffentlichkeit nicht wahrgenommen worden.

Der LfD steht zumindest dem Einsatz privater Sicherheitsdienste durch kommunale Ordnungsämter in der beschriebenen Form zurückhaltend gegenüber. Ohne ausdrückliche gesetzliche Regelung sprechen unabhängig von der sicherlich berechtigten Frage nach der Geeignetheit und Erforderlichkeit derartiger Maßnahmen auch Gesichtspunkte des Datenschutzes gegen eine solche Einbindung Privater in die originär dem Staat zugewiesenen Aufgaben. Denn hier erheben bzw. übermitteln die ausdrücklich mit der Wahrnehmung kommunaler Ordnungsaufgaben beauftragten Privaten zur Vorbereitung eines möglicherweise in Betracht kommenden staatlichen Einschreitens auch planmäßig und zielgerichtet personenbezogene Daten. Für die Übertragung dieser dem hoheitlichen Funktionsbereich zuzuordnenden Aufgaben auf private Stellen ist aber nach der Rechtsprechung des Bayerischen Obersten Landesgerichtes (Beschluss vom 5. März 1997; NJW 1997, 3454), die der LfD inhaltlich für richtig hält, eine gesetzliche Ermächtigung erforderlich.

18.3 Novellierung des Brand- und Katastrophenschutzgesetzes

Mit der am 1. Juli 2005 in Kraft getretenen Änderung des Brand- und Katastrophenschutzgesetzes konnte der LfD endlich eine bereichsspezifische Bestimmung zur Verarbeitung personenbezogener Daten durch die mit der Durchführung des LBKG beauftragten Stellen erreichen. Hervorzuheben ist in diesem Zusammenhang die dabei neu geschaffene ausdrückliche Regelung zur Aufzeichnung von Notrufen. Zwar war auch schon zuvor die datenschutzrechtliche Zulässigkeit der automatischen Aufzeichnung von Notrufen allgemein anerkannt (vgl. 15. Tb., Tz. 23.5); aus der Sicht des LfD bestand jedoch hinsichtlich Umfang, Verwendungszweck und Aufbewahrungsdauer der dabei anfallenden personenbezogenen Daten Regelungsbedarf.

§ 39 Abs. 4 LBKG stellt die Befugnis zur automatischen Aufzeichnung von Gesprächen, die über Notrufleitungen erfolgen, fest. Erfasst sind dabei alle Gespräche, die auf einem für die Entgegennahme von Notrufen vorgesehenen Leitstellenanschluss geführt werden. Die Aufzeichnungen dürfen grundsätzlich nur zur Durchführung und Abwicklung des Einsatzauftrages und zur Beweissicherung genutzt werden. Dies umfasst auch die Nutzung der Aufzeichnungen zur Aufklärung einer missbräuchlichen Verwendung des Notrufs. Angesichts der grundsätzlich schutzbedürftigen Informationen, die in den Aufzeichnungen enthalten sind, ist eine darüber hinausgehende Nutzung der Daten lediglich zur Evaluation oder zur Verfahrensverbesserung zulässig, wobei nach der Gesetzesbegründung hierzu im Regelfall aber die Verarbeitung anonymisierter Daten ausreichen dürfte. Zu beachten ist, dass nach der Regelung des § 39 Abs. 5 Satz 2 1. Halbsatz LBKG der Personenbezug der Daten, selbst wenn dieser bei der Heranziehung der Aufzeichnungen zu Zwecken der Qualitätssicherung ausnahmsweise erforderlich wäre, spätestens nach sechs Monaten gelöscht werden muss. Denn eine darüber hinausgehende längere personenbezogene Aufbewahrung der Daten ist lediglich zur Beweissicherung, nicht aber zur Evaluation oder Verfahrensverbesserung zulässig. Soweit die Aufzeichnungen wissenschaftlich genutzt werden sollen, sind die Daten immer vorab zu anonymisieren.

Im Hinblick auf die Löschung der Notrufaufzeichnungen hielt der LfD die in § 39 Abs. 5 LBKG vorgesehene Aufbewahrungsdauer von sechs Monaten auch unter Beachtung des Erforderlichkeitsgrundsatzes noch für vertretbar. Gerade angesichts möglicherweise im Einzelfall in Betracht kommender Ermittlungen durch die Staatsanwaltschaft, des Trägers der Leitstelle oder der Aufsichtsbehörde, die nach Darstellung des ISM regelmäßig erst mit einer deutlichen zeitlichen Verzögerung in Gang kommen, war die ursprünglich vom LfD als angemessen gehaltene Speicherfrist von sechs Wochen (vgl. 15. Tb., Tz. 23.5) nicht mehr aufrecht zu erhalten. Nach § 39 Abs. 5 Satz 2 LBKG ist eine über den Zeitraum von sechs Monaten hinausgehende personenbezogene Aufbewahrung der Daten dagegen nur in Ausnahmefällen zu Zwecken der Beweissicherung in einem konkreten Verfahren zulässig.

18.4 Abfallschuldner gesucht!

Um auch den letzten potentiellen Abfallschuldner aufzuspüren, kam eine Kreisverwaltung auf die Idee, bei den Verbandsgemeinden um Mitteilung der Personen zu bitten, die sich aus den der Verbandsgemeinde im Zusammenhang mit der möglichen Ausübung des gemeindlichen Vorkaufsrechts vorgelegten notariellen Grundstückskaufverträgen als Grundstückserwerber ergeben. Die Verbandsgemeinde sollte auf einem bereits vorgefertigten Formular u. a. Name und Anschrift des „neuen Grundstückseigentümers" sowie den Zeitpunkt des Eigentümerwechsels eintragen und diese Daten an die Kreisverwaltung zur Änderung der dort geführten Abfallgebührenkartei weiterleiten. Nach Auffassung der Kreisverwaltung war die Verbandsgemeinde hierzu zumindest aufgrund einer Regelung der Abfallwirtschaftssatzung des Kreises rechtlich verpflichtet. Die Verbandsgemeinde bezweifelte dennoch die datenschutzrechtliche Zulässigkeit der erbetenen Datenweitergabe und bat den LfD um Rat.

Eine bereichsspezifische Rechtsgrundlage war weder für die Datenerfassung durch die Verbandsgemeinde noch für die Datenübermittlung an die Kreisverwaltung ersichtlich. Die das gemeindliche Vorkaufsrecht betreffenden Regelungen der §§ 24 ff. BauGB lassen lediglich eine Weiterleitung des Inhalts des Grundstückskaufvertrages an die Gemeinde zu. Weitergehende Übermittlungsbefugnisse an andere Stellen sind dagegen nicht enthalten. Darüber hinaus konnte auch nicht die Abfallwirtschaftssatzung des Landkreises als Grundlage für die erbetene Datenverarbeitung herangezogen werden, da zu den darin genannten von den Verbandsgemeindeverwaltungen zu erbringenden Unterstützungsmaßnahmen gerade nicht die Speicherung und Übermittlung der aus den notariellen Kaufverträgen stammenden Erwerberdaten gehören.

Soweit die allgemeine Regelung des § 13 Abs. 1 und Abs. 2 LDSG im Hinblick auf die Erfassung der Käuferdaten durch die Verbandsgemeindeverwaltung in Betracht kam, war bereits fraglich, ob die Speicherung dieser Daten noch für die Erfüllung der der Verbandsgemeinde obliegenden Aufgaben erforderlich war. Denn gerade im Zusammenhang mit der Abfallentsorgung fehlt es an einer derartigen gemeindlichen Aufgabenzuweisung. Zudem wäre die Erfassung der Käuferdaten durch die Verbandsgemeinde zum Zwecke ihrer Weiterleitung an die Kreisverwaltung als zweckändernde Datenspeicherung gemäß § 13 Abs. 2 LDSG zu qualifizieren. Die darin enthaltenen Zulässigkeitsvoraussetzungen lagen jedoch im konkreten Fall nicht vor. Insbesondere im Hinblick auf die in den §§ 13 Abs. 2 Nr. 1, 12 Abs. 4 Nr. 6 LDSG enthaltene Regelung war es nicht offensichtlich, dass die Erfassung der Käuferdaten im Interesse der Betroffenen lag, da zum Zeitpunkt der Datenspeicherung weder der notarielle Kaufvertrag geschlossen noch der Betroffene schon Grundstückseigentümer bzw. Gebührenschuldner ist. Im Ergebnis fehlte es somit bereits für die Speicherung der Käuferdaten durch die Verbandsgemeinde an der erforderlichen Rechtsgrundlage.

Aber auch eine direkte Weiterleitung der von der Kreisverwaltung erbetenen Informationen ohne Zwischenspeicherung durch die Verbandsgemeindeverwaltung – beispielsweise durch Übersendung kopierter Seiten – begegnete angesichts der in § 14 Abs. 1 Nr. 1 LDSG enthaltenen Voraussetzung datenschutzrechtlichen Bedenken. Denn die Weiterleitung von Daten möglicher zukünftiger Grundstückseigentümer bzw. potentieller Gebührenschuldner ist weder für die Erfüllung von Aufgaben der Verbandsgemeinde noch der der Kreisverwaltung erforderlich. Auch hierbei ist wieder zu berücksichtigen, dass zum Zeitpunkt der Datenübermittlung die hiervon Betroffenen weder Grundstückseigentümer noch Gebührenschuldner sind und sie auch noch nicht der in der Abfallwirtschaftssatzung des Kreises enthaltene Anschlusszwang trifft. Erst zum Zeitpunkt der Grundbucheintragung wäre dies der Fall.

Die Kreisverwaltung sah angesichts dieser Bewertung von entsprechenden Übermittlungsgesuchen gegenüber den Verbandsgemeinden des Kreises ab.

18.5 Einwilligungserklärung zur Weitergabe personenbezogener Daten im Zusammenhang mit einer Geburtsanzeige

Im Rahmen einer Eingabe wurde der LfD auf ein Formular aufmerksam gemacht, das zur standesamtlichen Anzeige der Geburt eines Neugeborenen von einem Krankenhaus eingesetzt wurde. In diesem Formular, das an das örtlich zuständige Standesamt adressiert war, befand sich ein mit „Einwilligung zur Weitergabe personenbezogener Daten" überschriebener Abschnitt. Darin hieß es weiterhin:

„Die Daten von Eltern und Kind werden nur im Amtsblatt der VG (…) veröffentlicht.

Uns ist bekannt, dass personenbezogene Daten durch den Standesbeamten nur an solche Stellen weitergegeben werden dürfen, die in den für ihn geltenden Vorschriften genannt sind.
Wir sind aber damit einverstanden, dass die Vor- und Familiennamen des Kindes und der Eltern sowie deren Anschrift der regionalen Tagespresse, den ortsansässigen Banken und Sparkassen, Versicherungen oder anderen interessierten Stellen weitergegeben werden. Uns ist bekannt, dass die Daten nach der Veröffentlichung auch für Werbezwecke, Meinungsforschung usw. verwendet werden und in Dateien von Firmen, Institutionen o. ä. gespeichert werden.
Uns ist bekannt, dass wir die Einwilligung mit Wirkung für die Zukunft widerrufen können.
Wir geben hiermit unsere ausdrückliche Einwilligung im Sinne des § 4 BDSG (Bundesdatenschutzgesetz) in der jetzt gültigen Fassung sowie der entsprechenden landesrechtlichen Bestimmung."

Wie sich herausstellte, stammte der Erklärungstext weitestgehend aus dem von den meisten Standesämtern verwendeten Standesamtsprogramm AUTISTA, dessen Herausgeber ein Verlag in Frankfurt/M. ist. Dieser erklärte gegenüber der Verbandsgemeindeverwaltung, dass der fragliche Text zur Veröffentlichung von Personenstandsfällen rechtlich abgeklärt sei.

Nach Ansicht des LfD entsprach die Einwilligungserklärung nur teilweise den gesetzlichen Anforderungen des § 5 Abs. 2 und 3 LDSG. Neben der nur unzureichend realisierten Hervorhebung des äußeren Erscheinungsbildes war unklar, ob es sich bei den beiden Textteilen (Veröffentlichung im Amtsblatt; allgemeine Weitergabe an Dritte) um Erklärungsalternativen handelt bzw. ob einzelne oder beide Möglichkeiten abgelehnt werden können. Im Hinblick auf die in § 5 Abs. 2 LDSG enthaltenen Aufklärungs- und Hinweispflichten fehlte es an einem deutlichen Hinweis auf die Freiwilligkeit der Einwilligungserklärung. Die Betroffenen wurden zudem weder über die Identität der für die Datenweitergabe verantwortlichen Stelle (Standesamt der Verbandsgemeinde) noch über den Zweck der angestrebten Datenverarbeitung (z. B. Unterrichtung der Öffentlichkeit, Durchführung von Werbemaßnahmen etc.) informiert. Auch der mögliche Empfängerkreis blieb sehr unbestimmt: regionale Tagespresse, ortsansässige Banken und Sparkassen, andere interessierte Stellen und Versicherungen ließen keine eindeutige Identifizierung des Empfängers zu. Die Betroffenen waren damit nicht in der Lage, die Reichweite ihrer Erklärung abzuschätzen. Schließlich war der am Ende der Einwilligungserklärung enthaltene Hinweis auf § 4 BDSG angesichts der hier heranzuziehenden Regelung des § 5 LDSG irreführend. Der Umstand, dass der Einwilligungstext aus dem deutschlandweit eingesetzten Standesamtsprogramm „AUTISTA“ übernommen wurde, führte zu keiner anderen Beurteilung, da sich die datenschutzrechtliche Bewertung der von rheinland-pfälzischen Standesämtern verwendeten Einwilligungserklärung ausschließlich nach den Vorgaben des § 5 LDSG richtet.

Das angesichts der grundlegenden Bedeutung der Angelegenheit eingebundene ISM teilte die getroffene datenschutzrechtliche Beurteilung und kündigte zugleich an, in Abstimmung mit dem LfD einen datenschutzgerechten Mustervordruck einer in diesem Zusammenhang einzusetzenden Einwilligungserklärung zu entwickeln.

18.6 Einsicht und Auskunft aus dem Liegenschaftskataster

Ein Petent problematisierte diverse Gesichtspunkte zur Verfahrensweise der Vermessungsbehörden im Zusammenhang mit der Übermittlung personenbezogener Geobasisinformationen aus dem Liegenschaftskataster. Einerseits bemängelte er, dass die Vermessungsbehörden vor Herausgabe der o. g. Daten an Personen und Stellen außerhalb des öffentlichen Bereichs den betroffenen Grundstückseigentümer grundsätzlich nicht anhören, obwohl die Regelung des § 13 Abs. 2 Nr. 2 LGVerm eine Datenübermittlung nur erlaube, wenn dadurch überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt würden. Diese Praxis der Vermessungsverwaltung verhindere eine Berücksichtigung der Interessen der von der Übermittlung Betroffenen und sei daher rechtswidrig. Weiterhin würden auf der Grundlage des § 13 LGVerm stattfindende Datenübermittlungen bei den Vermessungsbehörden des Landes nicht aktenkundig gemacht, so dass eine nachträgliche Überprüfung ihrer Zulässigkeit faktisch unmöglich sei.

Das vom LfD eingebundene ISM hielt unter Hinweis auf die Regelung in Nr. 1.5.3 der Verwaltungsvorschrift „Übermittlung und Verwendung der Geobasisinformationen des amtlichen Vermessungswesens“ (VV-Übermittlung-GeoBasis) die regelmäßige Durchführung einer verwaltungsverfahrensrechtlichen Anhörung vor Übermittlung personenbezogener Geobasisinformationen an Personen oder Stellen außerhalb der Verwaltung nicht für geboten. Gleichzeitig bestätigte das Ministerium, dass mündlich vorgetragene Anträge auf Gewährung von Einsichtnahme oder auf eine mündliche Auskunftserteilung bislang in der Regel nicht aktenkundig gemacht werden.

In seiner datenschutzrechtlichen Bewertung differenzierte der LfD:

Soweit das ISM vor Übermittlung personenbezogener Geobasisinformationen durch die Vermessungsverwaltung die regelmäßige Durchführung von Anhörungsverfahren ablehnt, bestehen hiergegen aus datenschutzrechtlicher Sicht keine Bedenken. Zwar setzt die in § 13 Abs. 2 Nr. 2 LGVerm enthaltene Regelung für die Vornahme der darin vorgesehenen Interessenabwägung die Kenntnis der schutzwürdigen Interessen der Betroffenen voraus. Dies bedeutet aber nicht, dass die Vermessungsverwaltung aufgrund der verwaltungsverfahrensrechtlichen Regelungen der §§ 1 LVwVfG; 28 VwVfG rechtlich verpflichtet wäre, diese schutzwürdigen Interessen der Betroffenen von Amts wegen zu ermitteln bzw. die Betroffenen vor der beabsichtigten Übermittlung regelmäßig anzuhören. Denn die Heranziehung dieser Regelungen setzt den bevorstehenden Erlass eines (belastenden) Verwaltungsaktes i. S. v. § 35 VwVfG voraus, was im Falle der nach § 13 Abs. 2 Nr. 2 LGVerm begehrten Einsichtnahme und Auskunftserteilung aber gerade nicht gegeben ist. Darüber hinaus enthält auch die in diesem Zusammenhang erlassene Verwaltungsvorschrift keine Regelung, die die Durchführung eines Anhörungsverfahrens zwingend gebietet. Nach Nr. 1.5.3 VV-Übermittlung-GeoBasis setzt die Berücksichtigung der schutzwürdigen Interessen der Betroffenen lediglich voraus, dass die übermittelnde Stelle über entsprechende konkrete Erkenntnisse verfügt, nicht aber, dass diese von ihr auch aktiv ermittelt werden. Angesichts des nach § 1 Abs. 2 LGVerm mit der Bereitstellung der Geobasisinformationen in einem Geobasisinformationssystem verfolgten Zwecks wäre auch dessen Funktionsfähigkeit in Frage gestellt, wenn vor jeder beabsichtigten Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereiches ein Anhörungsverfahren durchgeführt werden müsste. Für den Betroffenen stellt dies keine rechtliche Benachteiligung dar, da er jederzeit der Vermessungsverwaltung die nach seiner Auffassung zu berücksichtigenden schutzwürdigen Interessen mitteilen kann.

Hinsichtlich der fehlenden Dokumentation der auf der Grundlage des § 13 Abs. 2 LGVerm erfolgten Datenübermittlungen hielt der LfD dagegen die bisherige Verfahrensweise der Vermessungsverwaltung für unzureichend. Denn einerseits sollte der von einer entsprechenden Datenübermittlung Betroffene schon aus Gründen der Transparenz die Möglichkeit haben, zuvor von der Vermessungsverwaltung durchgeführte Weitergaben ihn betreffender Geobasisinformationen und insbesondere die dabei von der

übermittelnden Stelle vorzunehmende Interessenabwägung nachvollziehen zu können. Daneben gebietet allerdings auch der in § 18 Abs. 3 LDSG enthaltene allgemeine Auskunftsanspruch, der sich u. a. auch auf den Empfängerkreis weitergegebener personenbezogener Daten bezieht, eine vollständige Dokumentation aller von der Vermessungsverwaltung an Dritte vorgenommenen Datenübermittlungen. Dies bedeutet, dass entgegen der jetzigen Verfahrensweise auch die durch die Servicestellen der Vermessungs- und Katasterämter auf der Grundlage einer persönlichen Vorsprache gewährten Einsichtnahmen und Auskünfte an Dritte aktenkundig gemacht werden müssen.

Das ISM als oberste Vermessungs- und Katasterbehörde wurde daher um entsprechende Änderung der gegenwärtigen Verwaltungspraxis gebeten.

18.7 Veröffentlichung kandidatenbezogener Auswertungen der Wahlergebnisse von Kommunalwahlen

Im Zusammenhang mit der Kommunalwahl 2004 interessierte sich ein Petent für die Veröffentlichung kandidatenbezogener Auswertungen der Wahlergebnisse, die beispielsweise die von den Wählern durchgeführten Streichungen betreffen. So wollte er in Erfahrung bringen, welche Kandidaten einer jeweiligen Liste in welcher Häufigkeit von den Wählern gestrichen wurden, um eine Hitliste der Kandidaten-Ergebnisse zu erstellen. Nachdem er von dem für ihn zuständigen Wahlamt abgewiesen wurde, bat er den LfD um Unterstützung seines Anliegens. Dem konnte leider nicht entsprochen werden.

Der Gesetz- und Verordnungsgeber hat in den einschlägigen Bestimmungen der §§ 40 ff. KWG bzw. §§ 63, 65 KWO abschließend geregelt, welche Inhalte als Wahlergebnis festzustellen sind. Das informationelle Selbstbestimmungsrecht der Wahlbewerber ist insoweit berechtigterweise eingeschränkt worden. Für darüber hinaus gehende kandidatenbezogene Auswertungen besteht dagegen kein Raum, so dass die gewünschte Veröffentlichung von Listen, aus denen die Häufigkeit der Streichungen einzelner Kandidaten ersichtlich wäre, zu Recht abgelehnt wurde. Der Petent wurde im Rahmen der Beantwortung seiner Eingabe darauf hingewiesen, dass der Gesetzgeber im Hinblick auf sonstige Wahlauswertungen, die nicht von den o. g. Regelungen erfasst sind, in § 73 KWG die Möglichkeit der nicht kandidatenbezogenen statistischen Auswertung vorgesehen hat. Nach Absatz 2 dieser Vorschrift können beispielsweise auch Untersuchungen über das Stimmverhalten der Wähler zur Feststellung, in welchem Umfang die Möglichkeiten des Kumulierens, Panaschierens und Streichens von Bewerbern genutzt wurden, als Landesstatistik erstellt werden. Eine auf einzelne Bewerber bezogene Auswertungsmöglichkeit ist aber auch in diesem Zusammenhang nicht vorgesehen.

18.8 Behördliche Schriftstücke auf der Straße

Ausnahmsweise können auch die Straßen des Landes aus datenschutzrechtlicher Sicht von besonderem Interesse sein. Diese Erkenntnis musste aus einem Vorfall in einer pfälzischen Ortschaft gezogen werden, nachdem sich auf der dortigen Hauptstraße mehrere behördliche Schriftstücke befanden und einem Passanten in die Hände fielen. Bei den Dokumenten handelte es sich um Kassenunterlagen, auf denen Namen und Kontonummern von Personen aufgelistet waren, die von der dortigen Kreisverwaltung Leistungen erhalten hatten. Auch die jeweilige Höhe der Zuwendung und der Verwendungszweck waren erkennbar.

Nach Rücksprache mit der betroffenen Kreisverwaltung stellte sich schnell heraus, dass die Schriftstücke im Rahmen eines von der Kommunalverwaltung durchgeführten Transports zur Aktenvernichtung verlorengegangen waren. Möglicherweise kamen die als vertraulich einzustufenden Dokumente versehentlich in einen für den Transport von nicht schutzbedürftigem Altpapier vorgesehenen unverschlossenen Behälter. Während der Fahrt löste sich dann die Plane des Fahrzeuganhängers und ermöglichte so den Verlust der Unterlagen.

Als Konsequenz aus dem Ereignis nahm die Kreisverwaltung diverse organisatorische Änderungen bei der Vernichtung von behördlichem Schriftgut vor. So werden diesbezügliche Unterlagen mit personenbezogenen Inhalten zunächst in abschließbaren Behältern gesammelt und täglich in einem zentralen Aktenvernichter zerkleinert, bevor sie dann zu dem mit der endgültigen Beseitigung beauftragten Unternehmen transportiert werden. Damit konnte die Kreisverwaltung die drohende Beanstandung des mit dem Vorfall verbundenen Verstoßes gegen datenschutzrechtliche Vorschriften abwenden.

19. Telekommunikation

19.1 Novellierung des Telekommunikationsgesetzes

Die notwendige Überarbeitung des Telekommunikationsgesetzes aufgrund europarechtlicher Vorgaben (vgl. 19. Tb., Tz. 19.1) wurde im Berichtszeitraum abgeschlossen. In Deutschland erfolgte die Umsetzung der Europäischen Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vom 12. Juli 2002 durch Inkrafttreten des Telekommunikationsgesetzes am 26. Juni 2004. Der Datenschutz ist nunmehr einheitlich im Siebten Teil des Telekommunikationsgesetzes geregelt und nicht mehr zusätzlich in einer Telekommunikations-Datenschutzverordnung, die vollständig in das Gesetz integriert wurde. Mit den neuen §§ 91 bis 107 TKG wird der Schutz personenbezogener Daten nun gesetzlich und nicht mehr nur durch Rechtsverordnung bestimmt. Im Zuge dieser begrüßenswerten Regelung, die auch auf eine Anregung der Datenschutzbeauftragten zurückgeht, wurden Vereinfachungen im Datenschutz erreicht und Doppelregelungen abgeschafft.

19.1.1 Änderungen bei der Speicherung der Verkehrsdaten

Die Verkehrsdaten (vor der Novellierung hießen sie Verbindungsdaten) dürfen jetzt im Regelfall bis zu sechs Monaten nach Rechnungsversand vollständig gespeichert werden. Bislang wurden die Zielrufnummern gem. § 7 Abs. 3 TDSV grundsätzlich um die letzten 3 Ziffern gekürzt gespeichert. Dieser Regelfall trat immer ein, wenn der Kunde nichts anderes gewählt hatte; eine datenschutzfreundliche Lösung, denn der Kunde musste nur dann aktiv werden, wenn er eine vollständige Speicherung der Verbindungsdaten oder deren vollständige Löschung nach Rechnungserstellung wünschte. In ihrer Entschließung vom 21. November 2003 (s. Anlage 1) kritisieren die Datenschuztbeauftragten des Bundes und der Länder, dass dieses Regel-Ausnahmeverhältnis mit der Novellierung umgekehrt wurde: Der Regelfall ist nun gem. § 97 Abs. 4 Satz 2 TKG die ungekürzte Speicherung der Verkehrsdaten.

Die Teilnehmer können aber auch künftig die um drei Stellen verkürzte Speicherung der Zielrufnummern nach § 97 Abs. 4 Satz 1 Ziff. 1 TKG sowie auch deren vollständige Löschung nach Versand der Rechnung gem. § 97 Abs. 4 Satz 1 Ziff. 2 TKG verlangen. Bei dieser Regelung handelt es sich um eine aus der Sicht des Datenschutzes nicht gerade ideale Widerspruchslösung; denn hier müssen die Kunden aktiv werden, um eine gekürzte Speicherung oder Löschung ihrer Daten nach Rechnungserstellung zu erreichen.

Immerhin hat sich der Bundesgesetzgeber im Einklang mit den wiederholt erhobenen Forderungen der Datenschutzbeauftragten (vgl. 19. Tb., Tz. 19.3) dafür entschieden, dass bei der Telekommunikation anfallende Verkehrsdaten nicht auf Vorrat für Strafverfolgungszwecke gespeichert werden dürfen. Gerade dies war bis zuletzt vom Bundesrat mit der Einführung einer gesetzlichen Pflicht der Anbieter zur Vorratsspeicherung aller Verkehrsdaten gefordert worden.

19.1.2 Datenerhebung beim Kauf von vertragslosen Handys – Vom Identifikationszwang beim Erwerb eines Prepaid-Produkts

Dieses problembeladene Thema hatte der LfD schon in seinem 19. Tätigkeitsbericht (Tz. 19.4) aufgegriffen und für eine anonyme Nutzungsmöglichkeit plädiert.

Zwischenzeitlich wurde durch Urteil des Bundesverwaltungsgerichtes vom 22. Oktober 2003 (Az. 6 C 23.02; NJW 2004, S. 1191) geklärt, dass § 90 Abs. 1 TKG a. F. keine ausreichende, dem Gebot der Normenklarheit genügende gesetzliche Grundlage für die Erhebung personenbezogener Kundendaten beim Erwerb vertragsloser Handys darstellte und demzufolge Anbieter von Mobilfunkleistungen nicht verpflichtet waren, beim Verkauf von Prepaid-Produkten personenbezogene Daten der Kunden zu erheben.

Daraufhin hat der Gesetzgeber im Rahmen der Novellierung in § 111 TKG die Pflicht zur Vorhaltung der Bestandsdaten für Auskunftsersuchen der Sicherheitsbehörden festgeschrieben. Sie trifft alle Anbieter (und damit auch alle Mobilfunkbetreiber), die geschäftsmäßig Telekommunikationsdienste erbringen und dabei Rufnummern vergeben.

Diese Regelung widerspricht den Vorgaben des Erwägungsgrundes 9 der Datenschutzrichtlinie für die elektronische Kommunikation (Richtlinie 2002/58/EG). Dort wird das Angebot anonymer und pseudonymer Telekommunikationsdienste gefordert, wobei es Ziel dieser Bestimmung ist, den Anspruch des Einzelnen auf informationelle Selbstbestimmung auch in der Telekommunikation zu stärken. Denn jeder Nutzer von Telekommunikationsdiensten soll selbst darüber bestimmen können, ob und wie viele seiner Daten er preisgeben möchte.

Damit ist es in Deutschland lediglich über den Weg öffentlicher Telefonzellen möglich, Telekommunikationsdienste anonym zu nutzen. Denn allein dort müssen sich die Anrufer (noch) nicht identifizieren.

19.1.3 Nutzung von Bestandsdaten zu Werbezwecken

Die Zulässigkeitsgrenzen für den Umgang mit Kundendaten zu Werbezwecken sind in § 95 Abs. 2 TKG geregelt.

Grundsätzlich dürfen Telekommunikationsdiensteanbieter die im Rahmen ihrer jeweiligen Vertragsverhältnisse anfallenden Teilnehmerdaten – die sog. Bestandsdaten – zur Werbung für eigene Angebote nur dann verwenden, wenn der Teilnehmer eingewilligt hat. Dies wird als „Opt-In-Lösung“ bezeichnet.

Im Rahmen einer bestehenden Kundenbeziehung darf der Diensteanbieter jedoch die Rufnummer sowie die Post- und E-Mail-Adresse zu Werbezwecken verwenden; wobei dies solange zulässig ist, bis der Kunde der Nutzung seiner Daten zu diesen Zwecken widersprochen hat. Hier gilt also das (kundenunfreundlichere) „Opt-Out-Prinzip“.

19.1.4 Mit der Inverssuche über die Rufnummer zu Name und Anschrift

Auskunftsdienste durften bislang nur Telefonnummer und Anschrift zum Namen eines Teilnehmers mitteilen. Seit dem In-Kraft-Treten des neuen Telekommunikationsgesetzes erhält man auch Auskunft über Namen und Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt ist (§ 105 Abs. 3 TKG). Eine solche Inverssuche ist allerdings nur dann zulässig, wenn der über seine Rufnummer angefragte Teilnehmer im Telefonbuch oder einem öffentlichen elektronischen Kundenverzeichnis mit den entsprechenden Daten eingetragen ist und dieser Art der Auskunft nicht widersprochen hat. Der Telekommunikationsdiensteanbieter muss seine Teilnehmer auf dieses Widerspruchsrecht – das nicht fristgebunden ist – hinweisen. Der Widerspruch kann also jederzeit erklärt werden.

19.1.5 Verarbeitung von Standortdaten im Mobilfunk

Entsprechend der Regelung in Artikel 9 der Datenschutzrichtlinie für elektronische Kommunikation wurden in § 98 TKG für den Bereich Mobilfunk die datenschutzrechtlichen Voraussetzungen für das Angebot standortbezogener Dienste („location-based-services“; vgl. hierzu auch 19. Tb., Tz. 19.1) geschaffen. Der Anwendungsbereich dieser ortsabhängigen Dienste, die dem Nutzer in Abhängigkeit von seinem aktuellen Aufenthaltsort zur Verfügung gestellt werden, reicht von Hinweisen auf die nächstgelegene Tankstelle, über freie Parkplätze bis hin zur lokalen Wettervorhersage. Um der Gefahr zu begegnen, dass hier ohne weiteres Bewegungsprofile erzeugt werden, ist grundsätzlich die Einwilligung der jeweiligen Kunden in die Lokalisierung notwendig.

19.2 EU-Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten

Das novellierte Telekommunikationsgesetz enthält ganz bewusst keine Regelungen zur Vorratsspeicherung (s. Tz. 19.1.1). Der Deutsche Bundestag hat diese Sichtweise in seinem Beschluss vom 17. Februar 2005 nochmals bekräftigt (vgl. BT-Drs. 15/4597).

Allerdings ist das Thema damit nicht vom Tisch. So könnte es über die Europäische Union auch in Deutschland zu einer Vorratsspeicherung von Kommunikationsdaten kommen.

Nach dem Terroranschlag in Madrid im März 2004 haben Frankreich, Irland, Schweden und Großbritannien dem EU-Ministerrat den Entwurf eines Rahmenbeschlusses vorgelegt, der vorsieht, dass alle Anbieter von Telekommunikations- und Internetdiensten zur Speicherung sämtlicher Daten über Nutzer dieser Dienste für einen Zeitraum von mindestens zwölf und maximal 36 Monaten verpflichtet werden können. (Offizielle Bezeichnung: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus vom 28. April 2004 – Ratsdokument 8958/04.)

Zum Hintergrund: Nach Art. 29 des EU-Vertrages verfolgt die Europäische Union das Ziel, ein gemeinsames Vorgehen der Mitgliedstaaten im polizeilichen und justiziellen Bereich herbeizuführen. Gemäß Art. 34 Abs. 2 lit. b) EU-V kann der Rat hierzu Rahmenbeschlüsse zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten fassen. Die Beschlüsse sind einstimmig zu treffen (vgl. Art. 34 Abs. 1 Satz 2 EU-V), wobei die Stimmenthaltung von anwesenden oder vertretenen Mitgliedern dem Zustandekommen der Beschlüsse nicht entgegensteht (Art. 23 Abs. 1 Satz 1 EU-V). Nur wenn das Ratsmitglied bei Stimmenthaltung eine förmliche Erklärung abgibt, ist es nicht verpflichtet, den Beschluss durchzuführen. Dies bedeutet: Um zu verhindern, dass die Regelungen eines EU-Rahmenbeschlusses in Deutschland verbindlich werden, müsste sich die Bundesregierung entweder ausdrücklich gegen darin aufgenommene Verpflichtungen aussprechen oder sich durch eine entsprechende förmliche Erklärung der Stimme enthalten.

Ziel des Vorschlages ist die Erleichterung der justiziellen Zusammenarbeit in Strafsachen, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsspeicherung angeglichen werden. Der Umfang der geplanten Datenspeicherung ist imponierend: Von dem Beschlussentwurf erfasst werden alle Verkehrsdaten der Telekommunikation im Fest- und Mobilfunk einschließlich der dazugehörigen Messaging-Dienste (SMS-Kurzmitteilungen), aber auch Standortdaten, die Grundlage für die Erbringung ortsabhängiger Dienste („location based services“) sind. Im Bereich des Internets sind u. a. Internet-Protokolle einschließlich E-Mail und WWW betroffen. Die Inhalte der Kommunikation werden nicht erfasst.

In einer gemeinsamen Presseerklärung vom 21. Juni 2004 – die nachfolgend wiedergegeben ist – haben sich die Datenschutzbeauftragten des Bundes und der Länder entschieden gegen diese Pläne zur umfassenden Vorratsspeicherung gewandt:

„Der Bundesgesetzgeber hat erst vor kurzem bei der Verabschiedung des neuen Telekommunikationsgesetzes aus gutem Grund die Einführung einer Pflicht zur Vorratsdatenspeicherung abgelehnt. Das grundgesetzlich garantierte Fernmeldegeheimnis lässt eine Speicherung von Daten über die Nutzung öffentlicher Telekommunikationsnetze (insbesondere auch des Internets) außer für betriebliche Zwecke nur zu, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung besteht. Zudem würde eine flächendeckende Vorratspeicherung von Kommunikationsdaten auch die Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen verletzen. Jede Auswertung von Internetadressen kann etwas über die Interessen, Vorlieben und politischen Präferenzen der Nutzenden verraten. Diese Adressen müssten nach dem Vorschlag für einen Rahmenbeschluss auf Vorrat gespeichert werden. Darüber hinaus bestehen erhebliche Zweifel, ob der vorgeschlagene Rahmenbeschluss mit Artikel 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privatlebens und der Korrespondenz) vereinbar ist. Der Europäische Gerichtshof für Menschenrechte hat betont, dass die Vertragsstaaten auch zur Bekämpfung des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten. Vielmehr muss es sich um Maßnahmen handeln, die in einer demokratischen Gesellschaft notwendig sind und dem Verhältnismäßigkeitsgrundsatz entsprechen. Die flächendeckende anlassunabhängige Speicherung aller Daten über die Nutzung öffentlicher Kommunikationsnetze schießt dagegen weit über das für die Vorbeugung und Verfolgung von Straftaten erforderliche Maß hinaus. Die Datenschutzbeauftragten fordern die Bundesregierung auf, den Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten über die Nutzung von öffentlichen elektronischen Kommunikationsdiensten und -netzen abzulehnen.“

Ebenso hat die Art. 29-Datenschutzgruppe (s. Tz. 3.3) den vorliegenden Entwurf für nicht akzeptabel erklärt und den EU-Ministerrat zur Ablehnung aufgefordert (vgl. Stellungnahme 9/2004 vom 9. November 2004, WP 99).

Desweiteren hat der Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder seine rechtlichen Bedenken gegen die Einführung einer Vorratsspeicherung von Verkehrsdaten in einer schriftlichen Stellungnahme im Rahmen eines von der EU-Kommission durchgeführten Konsultationsverfahrens dargelegt. Diese umfassende Stellungnahme ist in der Anlage 17 nachgewiesen.

Schließlich hat das Europäische Parlament in seiner Sitzung vom 7. Juni 2005 den Beschlussvorschlag zur Vorratsspeicherung von Kommunikationsdaten abgelehnt. Juristische Probleme würden Art. 8 der Europäischen Menschenrechtskonvention sowie nationale Verfassungen und Grundrechte bereiten; wie etwa das in Deutschland geltende Grundrecht auf informationelle Selbstbestimmung oder das Fernmeldegeheimnis. Was die Rechtfertigung der Datenspeicherung anbelangt, müsse der Mehrwert dargelegt werden, warum es notwendig sei, in den öffentlichen Telekommunikationsnetzen (Internet, Telefon, Mobiltelefon) die Daten von 450 Millionen Menschen grundsätzlich auf Vorrat zu speichern.

19.3 Öffentliche Arbeitgeber als Telekommunikationsunternehmen

Datenschutzrechtliche Probleme im Zusammenhang mit der Internet- und E-Mail-Nutzung durch Bedienstete hatte der LfD bereits im 18. Tb., Tz. 17.4 angesprochen. Erlaubt eine Behörde nur die dienstliche Nutzung von Internet und E-Mail, ist sie weder Telekommunikationsanbieter im Sinne des Telekommunikationsgesetzes noch Teledienstanbieter im Sinne des Teledienstegesetzes. Somit ist die Kontrolle der Internet- und E-Mail-Nutzung im Rahmen der Erforderlichkeit zulässig. Gegen eine Protokollierung der Zugriffe der Bediensteten mit Tag, Uhrzeit, Beginn und Dauer der Internetnutzung sowie der Absender- und Zieladressen bestehen aus datenschutzrechtlicher Sicht keine grundsätzlichen Einwände.

Gestattet der Dienstherr auch die private Nutzung von Internet und E-Mail, so muss er sich vielfältigen Rechtsproblemen stellen. Da der öffentliche Arbeitgeber damit gegenüber seinen Bediensteten zum Diensteanbieter wird, hat er u. a. die Vorschriften des Telekommunikationsgesetzes zu beachten und ist somit gem. § 88 TKG zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Gemäß § 206 Abs. 1 StGB wird die Verletzung des Fernmeldegeheimnisses dann unter Strafe gestellt, wenn es sich um Unternehmen handelt, die geschäftsmäßig Telekommunikationsdienste erbringen. In diesem Zusammenhang sei auf eine Gerichtsentscheidung hingewiesen, bei der es um die Strafbarkeit des Ausfilterns elektronischer Post ging. Ausgangspunkt des Verfahrens war die Strafanzeige eines ehemaligen Mitarbeiters einer Universität. Nachdem er ausgeschieden war, hatte er per elektronischer Post weiter mit dort tätigen Bediensteten Kontakt gehalten. Die Hochschule verbot ihm dann, weiterhin ihre Kommunikationseinrichtungen zu nutzen. Alle an ihn gerichteten und von ihm stammenden Nachrichten wurden zentral ausgefiltert. Allerdings hatte die Universität darüber anfänglich weder ihn noch die anderen Beteiligten informiert. Hier hat nun das OLG Karlsruhe mit Beschluss vom 10. Januar 2005 (Az. 1 Ws 152/04; MMR 2005, S. 178) klargestellt, dass auch eine Hochschule als Unternehmen zu betrachten ist, wenn sie nicht ausschließlich hoheitlich tätig wird. Das ist dann der Fall, wenn sie die EDV-Systeme ihren Mitarbeitern zum Austausch von elektronischer Post für private Zwecke zur Verfügung stellt. Nicht nur wer fremde Nachrichten heimlich ausspäht, verletzt das Fernmeldegeheimnis, sondern – so das OLG Karlsruhe – auch derjenige, der etwa als Serverbetreiber elektronische Botschaften unwillkommener Absender für Dritte gezielt unterdrückt, ohne dass die Empfänger davon wissen und damit einverstanden sind.

Diese Rechtsauffassung kann allgemein im Bereich elektronischer Kommunikation zu schwer wiegenden Konsequenzen für öffentliche Stellen führen. Fraglich ist insbesondere, ob das Instrument der Einwilligung des Betroffenen in die Protokollierung seiner privaten Nutzung das Problem hinsichtlich der Einhaltung des Fernmeldegeheimnisses löst. Denn an der Kommunikation können Dritte beteiligt sein, die nicht darin eingewilligt haben, dass ihre durch das Fernmeldegeheimnis geschützte Kommunikation beim Empfänger protokolliert wird.

Ein Weg aus dieser Sackgasse ist der Verzicht auf die private Nutzung von E-Mail; denn die rein dienstliche Nutzung von elektronischer Post unterliegt nicht dem Fernmeldegeheimnis. Als „ Ausweichmodell“ würde es sich nach Auffassung des LfD anbieten, öffentlichen Stellen des Landes zu empfehlen, ihren Bediensteten zum Abruf und Versenden privater Mails die Nutzung sog. Free-Mail-Anbieter im Internet zu gestatten. Beim Abruf elektronischer Post über das Internet wäre der Kommunikationspartner – der Dritte – nicht mehr betroffen, da dann lediglich protokolliert würde, dass der Bedienstete die Seite eines Free-Mail-Anbieters aufgerufen hat.

Auf diese Möglichkeit hatte der LfD bereits im Rahmen seiner Stellungnahme zu der vom ISM entwickelten Musterdienstanweisung hingewiesen. Die verantwortlichen Stellen werden zu prüfen haben, ob sie ihre internen Regelungen an diese Entwicklung anpassen.

19.4 Dürfen Provider dynamische IP-Adressen speichern?

Darüber wird seit geraumer Zeit unter den Datenschutzbeauftragten und den Aufsichtsbehörden diskutiert. Anlässlich einer aktuellen Gerichtsentscheidung gab es einige Presseanfragen, wobei der LfD auf Folgendes hingewiesen hat:

Im Internet sind Rechner nur unter einer eindeutig definierten Internet-Protokolladresse (IP-Adresse) erreichbar. Insbesondere Privatanwender verbinden ihren Rechner in der Regel nicht dauerhaft, sondern nur bei Bedarf mit dem Internet. In diesen Fällen wird dem Nutzer eine IP-Adresse vom Provider für die Dauer der jeweiligen Verbindung dynamisch zugewiesen. Im Unterschied zu sta-

tischen IP-Adressen – die dauerhaft einem bestimmten Rechner zugewiesen sind – können diese dynamischen, für die Dauer einer „Sitzung“ jeweils neu vergebenen IP-Adressen immer wieder von völlig unterschiedlichen Rechnern und Anschlussinhabern verwendet werden. Die dynamische IP-Adresse ist also kein Bestands-, sondern ein Verkehrsdatum.

Der Access-Provider (Zugangsanbieter) ist gem. § 96 Abs. 1 TKG berechtigt, Verkehrsdaten zu speichern. Gemäß § 96 Abs. 2 TKG ist eine Verwendung nach Ende der Verbindung nur in den dort genannten Ausnahmefällen zulässig. Dies betrifft die Entgeltermittlung, den Einzelverbindungsnachweis sowie Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten. Ob die Access-Provider anlassunabhängig zur Speicherung der dynamischen IP-Adressen nach Beendigung der Nutzung in einer Logdatei berechtigt sind, ist umstritten. So wird beispielsweise Kunden von T-Online bei der Einwahl ins Internet eine IP-Adresse dynamisch zugeteilt. Die Daten, wem zu welchem Zeitpunkt welche Adresse zugeteilt wurde, werden dort mehrere Monate gespeichert. Dagegen klagte ein Kunde vor dem Amtsgericht Darmstadt, das diese Datenspeicherung für unzulässig erklärte. In seinem Urteil vom 30. Mai 2005 (Az.: 300 C 397/04) vertritt das Gericht die Auffassung, dass die IP-Adresse insbesondere nicht für Abrechnungszwecke erforderlich ist. Der klagende T-Online-Kunde wurde in seiner Auffassung, dass es sich bei der Speicherung dynamischer IP-Adressen um eine unzulässige Maßnahme handele, durch ein Gutachten des Bundesbeauftragten für den Datenschutz unterstützt.

20. Medien

20.1 Entwurf eines Telemediengesetzes

Im November 2004 haben sich Bund und Länder auf Eckpunkte zur Fortentwicklung der Medienordnung verständigt (vgl. hierzu 19 Tb., Tz. 20.1). Mit dem dort erstmals verwendeten Begriff der Telemedien wird die wenig praxistaugliche Abgrenzung zwischen Teleddiensten und Mediendiensten aufgehoben. Dementsprechend sollen das Teledienstegesetz und Teledienstedatenschutzgesetz des Bundes sowie der Mediendienstestaatsvertrag der Länder durch ein Telemediengesetz des Bundes abgelöst werden, in dem allgemeine rechtliche Anforderungen an die Dienste festgelegt werden sollen. Für datenschutzrechtliche Bestimmungen ist ein eigenes Kapitel vorgesehen. Was den Geltungsbereich anbelangt, soll klargestellt werden, dass für die Internetzugangsvermittlung (access-providing) die Datenschutzregelungen des Telekommunikationsgesetzes gelten.

Eine Bund-Länder-Arbeitsgruppe, an der auch Vertreter der Datenschutzbeauftragten des Bundes und der Länder teilnehmen, wurde beauftragt, entsprechende Gesetzentwürfe zu erarbeiten. Ein wichtiges datenschutzrechtliches Anliegen ist es, auch für den Bereich der Telemedien-Dienste eine Geheimhaltungsvorschrift nach dem Vorbild des Fernmeldegeheimnisses (§ 88 TKG) in das Gesetz aufzunehmen. Ein solches Mediennutzungsgeheimnis entspricht einer seit Jahren erhobenen Forderung der Datenschutzbeauftragten. Bereits zu Beginn der Beratung über eine neue Medienordnung im Jahre 2001 hat die 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich die Einführung eines einfachgesetzlichen umfassenden Mediennutzungs- und Kommunikationsgeheimnisses in einer Entschließung gefordert. Die Einführung eines Mediennutzungsgeheimnisses entspricht auch der angestrebten EU-konformen Fortentwicklung des Datenschutzrechts. Artikel 5 Abs. 1 der Richtlinie 2002/58/EG verpflichtet die Mitgliedstaaten, die Vertraulichkeit der elektronischen Kommunikation durch innerstaatliches Recht sicherzustellen. Die Richtlinie unterscheidet dabei nicht zwischen Telekommunikation und anderen elektronischen Informations- und Kommunikationsdiensten.

20.2 Änderung des Rundfunkgebührenstaatsvertrages – Kauf von Adressdaten durch die GEZ

Die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland (GEZ) ist eine Gemeinschaftseinrichtung der ARD-Landesrundfunkanstalten, des Deutschlandradios und des Zweiten Deutschen Fernsehens. Die GEZ nimmt als Rechen- und Servicezentrum für die Rundfunkanstalten alle mit der Gebührenzahlung zusammenhängenden Aufgaben wahr. Sie speichert und verarbeitet die Daten der Rundfunkteilnehmer. Dabei wird sie als Abteilung der jeweiligen Landesrundfunkanstalt tätig. In Rheinland-Pfalz ist dies der Südwestrundfunk, für den der LfD nicht zuständig ist, denn die Aufgabe der datenschutzrechtlichen Kontrolle des Südwestrundfunks obliegt dem dortigen Rundfunkbeauftragten für den Datenschutz. Da sich der Rundfunkänderungsstaatsvertrag Anfang 2005 in der Gesetzesberatung der Länder befand, hielt es der LfD für geboten, die Kommission beim Landesbeauftragten für den Datenschutz allgemein über den datenschutzbezogenen Hintergrund der aktuellen Diskussion zum Kauf von Adressdaten durch die GEZ zu informieren.

Die für ihre Aufgaben notwendigen Daten erhält die GEZ zum einen von den Rundfunkteilnehmern selbst; zum anderen teilen die Meldebehörden der GEZ mit, wenn eine volljährige Person zuzieht, wegzieht oder verstirbt. Darüber hinaus beschafft die GEZ Daten beim kommerziellen Adresshandel. Diese bisher nur tolerierte Praxis ist nunmehr durch eine Änderung des Rundfunkgebührenstaatsvertrages, dem der Landtag durch Gesetz zugestimmt hat, legalisiert worden. So wurde § 8 um einen vierten Absatz erweitert. Danach dürfen die Rundfunkanstalten „zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt oder im Rahmen des Einzugs der Rundfunkgebühren entsprechend § 28 des Bundesdatenschutzgesetzes personenbezogene Daten erheben, verarbeiten oder nutzen.“

§ 28 BDSG regelt allerdings die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen für eigene Zwecke. Hier ist zunächst darauf hinzuweisen, dass die Landesrundfunkanstalten verpflichtet sind, die ihnen nach den Bestimmungen des Rundfunkgebührenstaatsvertrages zustehenden Gebühren möglichst vollständig einzuziehen. Um ihren Ver-

pflichtungen nachzukommen, haben sie in der Vergangenheit häufig das Instrument der Überprüfung durch Außendienstmitarbeiter genutzt. Auf der Suche nach einem für die Bürgerinnen und Bürger weniger einschneidenden Weg, als den der Überprüfung an der Haustür, hat die GEZ in den letzten Jahren Adressen gekauft, mit ihrem Bestand abgeglichen und dann diejenigen angeschrieben, die nicht bei ihr gemeldet waren. Diese Mailing-Aktionen wurden wegen der fehlenden Rechtsgrundlage vielfach kritisiert. Um in dieser Hinsicht Rechtssicherheit zu schaffen, hat der Gesetzgeber – wie oben beschreiben – die Forderung nach einer Rechtsgrundlage aufgenommen und den Adressenkauf im Rundfunkgebührenstaatsvertrag geregelt. Die dortige Bezugnahme auf die Verarbeitungsbefugnisse des § 28 BDSG wird allgemein als wenig glücklich erachtet. Von einigen Landesdatenschutzbeauftragten – die in ihren Bundesländern (anders als in Rheinland-Pfalz) für die dortige Rundfunkanstalt zuständig sind – wird diese Regelung als Erlaubnis zum Adresshandel gerügt. Soweit ersichtlich, haben die Landesrundfunkanstalten bzw. die GEZ jedoch zu keinem Zeitpunkt Handel mit Daten von Rundfunkteilnehmern betrieben. Vielmehr kauft die (öffentliche Stelle) GEZ von Adressanbietern Anschriften, und zwar ausschließlich für Mailing-Aktionen. Diese Daten werden nach Abschluss der Aktion, wenn sich hieraus kein Teilnehmerverhältnis ergeben hat, gelöscht.

Im Hinblick auf die Verhandlungen zum 9. Rundfunkänderungsstaatsvertrag sind bereits Formulierungsvorschläge für eine Neufassung des § 8 Abs. 4 Rundfunkgebührenstaatsvertrag an die Staatskanzleien herangetragen worden, um eine detaillierte, zweckorientierte (und weniger missverständliche) Regelung zum Adresskauf durch die GEZ zu verankern. Insbesondere sollte statt eines Verweises auf § 28 BDSG eine Vollregelung aufgenommen werden.

20.3 Fallstricke beim Betrieb eines Internetforums

Es liegt im Trend, auch bei öffentlichen Stellen in die Homepage ein Forum zu integrieren, das als virtueller „Marktplatz“ für die Bürgerinnen und Bürger dienen soll. In aller Regel kann jede interessierte Person, ohne ihre Identität preiszugeben, sich an dem Forum beteiligen. Mitunter entwickelt sich bald ein reger Meinungsaustausch zu allerlei – meist ortsbezogenen – Themen, in dessen Verlauf die Gemüter sich gelegentlich erhitzen und es zu ehrverletzenden Äußerungen und rufschädigenden Unterstellungen gegenüber einzelnen Personen kommen kann. Das gleiche gilt für Eintragungen in einem auf der Homepage zur Verfügung gestellten Gästebuch. Im Internet kann ein weltweit unbestimmter Personenkreis auf diese Daten zugreifen, so dass für die betroffenen Personen u. a. die Gefahr besteht, dass diskriminierende personenbezogene Daten bzw. personenbezogene Werturteile eine Prangerwirkung auslösen.

Zur Frage, inwieweit der Betreiber eines Forums oder Gästebuchs für Inhalte, die er nicht selbst eingestellt hat – also für fremde Inhalte – verantwortlich ist, enthalten der Mediendienstestaatsvertrag und das Teledienstegesetz inhaltlich deckungsgleiche Regelungen. Daher kann in diesem Zusammenhang dahinstehen, ob ein Teledienst oder ein Mediendienst vorliegt. So sind nach der Bestimmung in § 6 Abs. 2 Satz 1 Mediendienstestaatsvertrag (entspricht § 8 Abs. 2 Teledienstegesetz) Diensteanbieter für fremde Informationen, zu denen sie z. B. den Zugang zur Nutzung vermitteln oder die sie für einen Nutzer speichern, nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Hier ist also ein Haftungsprivileg für die Diensteanbieter geschaffen worden. Allerdings bleiben nach § 6 Abs. 2 Satz 2 der vorgenannten Regelung die Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen (z. B. nach dem Landesdatenschutzgesetz) unberührt.

Soweit über ein Forum oder ein Gästebuch persönliche Daten Betroffener „veröffentlicht“ werden, sind auch die einschlägigen Datenschutzvorschriften zu beachten. Zu diesen persönlichen Daten gehören neben der Nennung des Namens einer Person weitere personenbezogene oder personenbeziehbare Einzelangaben über persönliche oder sachliche Verhältnisse. Jede Form der Bereitstellung im Internet ist unter den Begriff der Verarbeitung personenbezogener Daten einzuordnen. Die Datenverarbeitung ist allerdings nur dann zulässig, wenn eine gesetzliche Grundlage vorhanden ist oder die Betroffenen eingewilligt haben, was bei den eingangs geschilderten Sachverhalten regelmäßig nicht der Fall ist, so dass die personenbezogenen Daten nach § 19 Abs. 2 Nr. 1 LDSG zu löschen sind.

Unabhängig von dieser Obliegenheit können sich Internet-Foren und -Gästebücher zu risikobehafteten Unternehmungen entwickeln. Gerade was die Verantwortlichkeit des Anbieters anbelangt, hat die Rechtsprechung das oben genannte Haftungsprivileg teilweise eingeschränkt:

Wer danach die Einträge über längere Zeit ungeprüft lässt, nimmt in Kauf, dass dort ehrverletzende Äußerungen über Dritte erscheinen. Er macht sich diese Eintragungen dadurch zu eigen. Ein allgemeiner Hinweis darauf, dass der Betreiber sich distanziere, reicht nicht aus, um diesen Eindruck zu verhindern (vgl. Landgericht Trier, Urteil vom 16. Mai 2001, Az.: 4 O 106/00). Eine Klausel, die einen Haftungsausschluss beinhaltet (Disclaimer), entlastet grundsätzlich nicht bezüglich der Haftung gegenüber geschädigten Dritten (OLG München, Urteil vom 17. Mai 2002, Az.: 21 U 5569/01). Nach einem Urteil des Landgerichts Düsseldorf vom 14. August 2002 (Az.: 2 a O 312/01) kann der Anbieter einer Haftung durch regelmäßige zeitnahe Kontrolle der Eintragungen im Forum (oder Gästebuch) entgehen, indem er dafür Sorge trägt, dass rechtsverletzende Äußerungen wieder gelöscht werden.

Um nicht in die Haftung zu geraten, sollten sich betroffene öffentliche Stellen also stets um die notwendige Pflege der Foren und Gästebücher kümmern.

Der LfD hat die Spitzenverbände der Städte und Gemeinden entsprechend unterrichtet.

21. Technischer und organisatorischer Datenschutz

21.1 Kontroll- und Beratungstätigkeit

Im Berichtszeitraum sind in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung in 87 Fällen örtliche Feststellungen und Beratungen unter technisch-organisatorischen Gesichtspunkten erfolgt, u. a. bei folgenden Stellen:

- AOK Rheinland-Pfalz,
- Arbeitsgemeinschaften nach § 44 b SGB II,
- Fachhochschulen,
- Finanzämtern,
- Fraunhofer Gesellschaft,
- Gesundheitsämtern,
- Gesellschaft für Kommunikation und Wissenstransfer KommWis GmbH,
- Kassenärztliche Vereinigung Rheinland-Pfalz,
- Kreisverwaltungen,
- Krankenhäusern,
- Kommunale Datenzentrale Mainz,
- Landespsychotherapeutenkammer,
- Landesbetrieb Daten und Information (LDI),
- Landesbetrieb Straßen und Verkehr,
- Landeskriminalamt,
- Ministerium für Bildung, Frauen und Jugend,
- Ministerium der Finanzen,
- Ministerium des Innern und für Sport,
- Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur,
- Ministerium für Arbeit, Soziales, Familie und Gesundheit,
- Polizeipräsidien,
- einer Polizeiinspektion,
- Rechenzentrum eines beauftragten Unternehmens,
- einer Sparkasse,
- einer Stadtverwaltung,
- Universitäten,
- Verbandsgemeinden,
- Zentralstelle für Polizeitechnik.

Ergänzt wurden diese durch dreizehn informatorische Feststellungen, überwiegend zur Klärung des technischen Verfahrensstands. Die Kontrollen erfolgten sowohl in Form allgemeiner Prüfungen als auch anlassbezogen unter ausgewählten Gesichtspunkten.

Die Praxis vieler Verwaltungen, den LfD im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder im Zusammenhang mit der Erstellung von Sicherheitskonzepten zu beteiligen, wurde beibehalten. Daneben wurden die Behörden und sonstigen öffentlichen Stellen des Landes und der Kommunen in zahlreichen technischen und organisatorischen Einzelfragen des Datenschutzes beraten.

Die Schulungsaktivitäten wurden im bisherigen Umfang fortgeführt.

21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren

21.2.1 Storage-Area-Network-Konzept des Landesbetriebs Daten und Information (LDI)

Der LDI beabsichtigt den Aufbau eines zentralen Storage Area Networks (SAN), das von unterschiedlichen Anwendungen genutzt werden kann. Hintergrund sind neben Kostenvorteilen, der Skalierbarkeit je nach Speicherplatzbedarf und der Aufwandsersparnis beim Betrieb Vorteile bei der Online-Sicherung von Datenbeständen. Kennzeichnend für derartige SAN-Lösungen ist die Zusammenführung der Datenhaltung verschiedener Anwendungs- bzw. Datenbanksysteme in Form gemeinsam genutzter netzwerkbasierter Speicher-Lösungen. Vor dem Hintergrund der Regelungen in § 9 Abs. 2 Nr. 3 und 8 LDSG bedarf es dabei Mechanismen, mit denen die vormalige Trennung der Speicherung angemessen nachgebildet werden kann.

Der LDI hat den Empfehlungen des LfD dadurch entsprochen, dass logische Speichereinheiten gebildet und einzelnen Servern dezidiert zugewiesen und innerhalb sogenannter Zonen Zugriffspfade fest definiert werden. Hinzu kommt eine Protokolltrennung zwischen lokalem Netz und Speichernetz auf der Netzwerkebene.

In bestimmten Fällen besteht bei der Datenspeicherung die Notwendigkeit, zum Schutz der Vertraulichkeit auch bei administrativen Zugriffen Daten zu verschlüsseln. Soweit dabei bislang hardwarebasiert Festplatten verschlüsselt wurden, besteht beim SAN des LDI die Möglichkeit, logische Speichereinheiten separat zu verschlüsseln.

Das SAN-Konzept des LDI begegnete aus datenschutzrechtlicher Sicht keinen Bedenken.

21.2.2 Landesdaten- und Kommunikationsnetz Rheinland-Pfalz (rlp-Netz)

Mit Beginn des Jahres 2005 wurde das technisch neustrukturierte Landesnetz in Betrieb genommen. Der LfD hat im Vorfeld der Ausschreibung der Netzleistungen zu den konzeptionellen Überlegungen Stellung genommen.

Im 19. Tätigkeitsbericht wurde unter Tz. 21.2.2.2 dargestellt, dass entgegen ursprünglicher Planungen die Kommunikation im rlp-Netz weiterhin nicht verschlüsselt wurde. Im Vorfeld der Neukonzeption des rlp-Netzes hat der LfD daher auf § 1 Abs. 2 des LDI-Errichtungsgesetzes hingewiesen. In Verbindung mit § 2 Abs. 2 Nr. 1 und 3 der LDI-Betriebssatzung obliegt dem Landesbetrieb danach die Gewährleistung einer sicheren Kommunikation innerhalb der Verwaltung.

Hierzu zählt angesichts geänderter Rahmenbedingungen aus Sicht des LfD die kryptografische Sicherung der Übertragungswege (vgl. 18. Tb., Tz. 21.2.2.2). In vergleichbaren Bereichen z. B. Kommunales Netz Rheinland-Pfalz, Informationsverbund Berlin-Bonn, TESTA-Netz hat sich eine Leitungsverschlüsselung als praktikabel erwiesen und wird standardmäßig genutzt. Angesichts der wachsenden Bedeutung des rlp-Netzes als zentrale Kommunikationsplattform der Landesverwaltung sollte aus Sicht des LfD daher auch für das Landesnetz generell die Möglichkeit einer kryptografisch gesicherten Kommunikation vorgesehen werden.

Der LDI hat dies bei der technischen Neugestaltung des rlp-Netzes berücksichtigt. Mit Aufnahme des Betriebs der neugestalteten Netzstruktur wurde in allen Bereichen des rlp-Netzes eine standardmäßige Verbindungsverschlüsselung eingeführt. Innerhalb des rlp-Netzes ist damit die Vertraulichkeit der Kommunikation gegenüber Dritten verlässlich gewährleistet. Einer langjährigen Forderung des LfD wurde damit entsprochen.

Als Ersatzlösung bei Ausfall von rlp-Netz-Leitungen sind alternative Verbindungen über öffentliche Kommunikationswege wie das Internet zu entsprechenden rlp-Netz-Gateways vorgesehen. Aus Sicht des LfD bestehen hiergegen keine Bedenken, wenn durch kryptografische Verfahren eine ausreichende Vertraulichkeit der Kommunikation, die Integrität der Daten und die Authentisierung der Teilnehmer gewährleistet wird; Wahl des Providers und Wegeführung sind in diesem Fall nachrangig. Auch die Anbindung von Telearbeitsplätzen oder Außenstellen sowie die Einrichtung alternativer Netzzugänge kann unter den genannten Voraussetzungen damit auch über das Internet erfolgen. Im Blick auf die Sicherheitsverantwortung des LDI für das rlp-Netz als Ganzes sollten entsprechende Lösungen allerdings nur im Rahmen einer Vereinbarung des LDI mit der betroffenen Verwaltung und mit vom LDI ausdrücklich unterstützten technischen Lösungen zugelassen werden.

21.2.3 Kommunales Netz Rheinland-Pfalz

Für das im Zusammenhang mit der Einführung des Verfahrens EWOIS-neu in Betrieb genommene Kommunale Netz Rheinland-Pfalz (vgl. 19. Tb., Tz. 21.2.4) sind substantielle Änderungen erfolgt, weitere sind geplant. Das Ziel ist dabei die technische und administrative Angleichung des Kommunalnetzes und des rlp-Netzes der Landesverwaltung. Der Umbau betrifft die Änderung der Netzstruktur, den Ersatz von Knotenrechnern und den Austausch der eingesetzten Verschlüsselungsgeräte.

Die bislang vom LDI wahrgenommenen administrativen Aufgaben sollen aufgeteilt werden, indem das Management der Knotenrechner künftig durch eine Tochterfirma des Anbieters der physikalischen Netzleitungen erfolgen soll. Die Administration der Verschlüsselungsboxen und damit die Kontrolle der Verbindungswege liegt weiterhin außerhalb der Kontrolle des Netzanbieters; dieser erhält Zugriff ausschließlich auf die verschlüsselte Kommunikation.

Der Umbau führt zu geringeren Kosten beim Betrieb des Netzes. Für die angeschlossenen Netzteilnehmer ergeben sich als Vorteile höhere Bandbreiten, die Möglichkeit der Priorisierung von Diensten sowie künftig die generelle Verschlüsselung der Kommunikation im Kommunalnetz. Nach der Umstellung des Kommunalnetzes erfolgt in Rheinland-Pfalz als bislang einzigem Bundesland generell und flächendeckend eine Verschlüsselung der Netzkommunikation im Bereich der Landes- und Kommunalverwaltung.

Aus den Änderungen ergeben sich keine inhaltlichen Auswirkungen auf die vom LDI wahrgenommenen Kontrollfunktionen. Aufgrund der dem LDI weiterhin obliegenden Administration der Verschlüsselungsgeräte im KNRP verbleibt, wie vom LfD gefordert, die Kontrolle der Verbindungswege ins rlp-Netz bei einer der Aufsicht des Landes unterliegenden öffentlichen Stelle. Der Netzumbau lässt weiterhin den Betrieb der Firewalls an den Netzübergängen zum rlp-Netz und zum Betreiber des EWOIS-Verfahrens unberührt. Angesichts dessen wurden vom LfD gegen den geplanten Netzumbau keine Bedenken erhoben.

21.2.4 Einwohnerinformationssystem Rheinland-Pfalz (EWOIS)

21.2.4.1 Kontrollmöglichkeiten des Landes beim Betrieb des Verfahrens durch eine nicht-öffentliche Stelle

Im 19. Tätigkeitsbericht wurde unter Tz. 21.2.5.6 dargestellt, welche Kontroll- und Aufsichtsfunktionen auf Anregung des LfD im Rahmen der Vergabe des EWOIS-Betriebs an eine nicht-öffentliche Stelle eingerichtet wurden.

Aus den unter Tz. 21.2.3 dargestellten Veränderungen im Kommunalnetz ergeben sich keine inhaltlichen Auswirkungen auf diese vom LDI wahrgenommenen Funktionen. Aufgrund der dem LDI auch weiterhin obliegenden Administration der Verschlüsselungsgeräte im KNRP verbleibt wie vom LfD gefordert die Kontrolle der Verbindungswege ins rlp-Netz bei einer der Aufsicht des

Landes unterliegenden öffentlichen Stelle. Der Netzumbau lässt auch den Betrieb der Firewalls an den Übergängen vom technischen Betreiber zum KNRP sowie vom KNRP zum rlp-Netz (Verbindungs- und Dienstekontrolle) unberührt. Angesichts dessen wurden vom LfD keine Bedenken erhoben.

21.2.4.2 Protokollierung von Abfragen im Informationssystem

Beim EWOIS-Informationssystem werden für Abrechnungszwecke und zur Datenschutzkontrolle Abfragen, Auswertungen sowie der Aufruf bestimmter Funktionen protokolliert. Die vorhandenen Mechanismen erlauben es dabei, den Umfang zu protokollierender Zugriffe variabel vorzugeben. Mit Aufnahme des Verfahrensbetriebs wurde eine Protokollierung von Gruppenabfragen zu 100 % und von Einzelabfragen zu 10 % Prozent eingestellt. Der LfD hatte im Vorfeld der Verfahrenseinführung darauf hingewiesen, dass aus seiner Sicht bei Einzelabfragen zumindest in bestimmten Bereichen die Notwendigkeit besteht, einen höheren Prozentsatz einzustellen.

Entgegen einer entsprechenden Zusage der betroffenen Stellen und des Verfahrensbetreibers war dies jedoch nicht erfolgt. Bei örtlichen Feststellungen hatte sich ergeben, dass weiterhin die o. g. Prozentsätze eingestellt waren. Auf der Grundlage dieser Protokolldaten war eine verlässliche Klärung erhobener Missbrauchsvorwürfe, d. h. des unbefugten Zugriffs auf Meldedaten, nicht möglich; diese konnten weder bestätigt noch entkräftet werden.

Damit hatte sich die für Einzelabfragen auf Stichproben reduzierte Protokollierung im Informationssystem für eine effektive Datenschutzkontrolle als unzureichend erwiesen. Angesichts eines Anteils der Einzelabfragen von mehr als zwei Dritteln der Gesamtzahl an Abfragen kann eine angemessene Nachvollziehbarkeit i. S. d. § 9 Abs. 2 Nr. 10 LDSG aus Sicht des LfD nur auf der Grundlage einer vollständigen Protokollierung auch der Einzelabfragen erfolgen.

In Abstimmung mit dem Betreiber ist zwischenzeitlich eine Anpassung des Verfahrens erfolgt. Nunmehr werden alle Abfragen im Informationssystem vollständig protokolliert, tageweise in verschlüsselter Form zur verfahrensbetreuenden Stelle des Landes, der KommWis GmbH, übermittelt und anschließend beim technischen Betreiber des Verfahrens gelöscht.

Den Empfehlungen des LfD wurde damit entsprochen.

21.2.5 Protokollierung von Zugriffen auf Internet-Angebote der Landesverwaltung

Wer im Internet unterwegs ist, hinterlässt Spuren; über Zeitpunkt, Art und Inhalt der Kommunikation, den genutzten Anschluss oder die Konfiguration des verwendeten PC. Manche dieser Informationen sind bereits direkt personenbezogen, andere lassen sich unter bestimmten Voraussetzungen individuell zuordnen. Zumeist erfolgt dies über die so genannte IP-Adresse, die dem PC eines Nutzers beim Internet-Zugriff zugeordnet wird. Die elektronischen Spuren finden sich in den Protokolldateien der Anbieter von Telekommunikations- und Telediensten, d. h. den Zugangs- bzw. Inhaltsanbietern.

Praktisch werden die meisten dieser Angaben benötigt, um die gewünschten Dienste, etwa den Zugriff auf eine Internet-Seite, erbringen zu können; vielfach dienen sie auch Abrechnungszwecken. Rechtlich handelt es sich zumeist um Nutzungsdaten nach § 6 Abs. 1 TDDSG; diese unterliegen nach § 8 Abs. 2 TDG dem Fernmeldegeheimnis.

Die datenschutzrechtlichen Risiken ergeben sich aus der Möglichkeit, aus den Protokolldaten unzulässige Kommunikations- oder Verhaltensprofile der Nutzer zu bilden. Dies gilt umso mehr, als die Angaben seitens der Anbieter vielfach herangezogen werden, um die Inanspruchnahme der angebotenen Dienste unter unterschiedlichen Gesichtspunkten auszuwerten oder um sie für Werbung zu verwenden.

Das TDDSG lässt daher eine Verarbeitung von Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus nur zu, soweit sie für Abrechnungszwecke erforderlich sind, sie anonymisiert bzw. pseudonymisiert werden oder die Nutzer in die Verarbeitung eingewilligt haben (§ 6 TDDSG). Angesichts des standardmäßigen Funktionsumfangs der eingesetzten Lösungen und einer häufig routinemäßig eingestellten Protokollierung bleibt vielfach jedoch fraglich, ob den Vorgaben des TDDSG in der Praxis entsprochen wird.

Viele Verwaltungen des Landes sind mit einem Informationsangebot im Internet vertreten und damit Anbieter von Tele- bzw. Mediendiensten (§ 2 Abs. 2 Nr. 2 TDG bzw. § 2 Abs. 1 MDStV). Sie greifen dabei in einer Reihe von Fällen auf den Landesbetrieb Daten und Information zurück, der im Rahmen des so genannten „Webserver-Hostings“ die technischen Dienstleistungen für Betrieb und Administration der eingesetzten Systeme erbringt. Verantwortlich im Sinne der medien- und datenschutzrechtlichen Vorschriften bleiben jedoch die auftraggebenden Verwaltungen.

Im Rahmen örtlicher Feststellungen ist der LfD der Frage nachgegangen, ob bei der Protokollierung von Zugriffen auf Internet-Angebote der Landesverwaltung die o. g. Vorgaben berücksichtigt werden.

Dabei hat sich ergeben, dass den Vorschriften des TDDSG nicht entsprochen wurde. Die Zugriffe auf die jeweiligen Internet-Angebote wurden standardmäßig für die Dauer von zwölf Monaten gespeichert, ohne dass dies für Abrechnungszwecke erforderlich war. Genutzt wurden die Daten lediglich für statistische Auswertungen, für die ein Personenbezug nicht benötigt wurde. Seitens

der auftraggebenden Verwaltungen waren in keinem Fall Vorgaben zur Speicherung oder Löschung der Nutzungsdaten erfolgt, obwohl die Speicherung regelmäßig in den Impressa der Internet-Angebote angesprochen wurde. Die Vorgaben des TDDSG für eine Speicherung von Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus wurden somit nicht eingehalten.

Da nach § 1 Abs. 2 TDDSG, soweit nichts anderes bestimmt ist, die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden sind, kommt nach mehrheitlicher Auffassung der Datenschutzbeauftragten neben den im TDDSG genannten Zwecken eine vorübergehende Speicherung von Nutzungsdaten für Zwecke der Datenschutzkontrolle, der Datensicherung oder der Sicherstellung eines ordnungsgemäßen Betriebs in Betracht (§ 9 Abs. 1 i. V. m. § 13 Abs. 6 LDSG).

Nach den Erfahrungen des LfD ist für diesen Zweck in der Regel eine Speicherung der Nutzungsdaten in personenbeziehbarer Form für die Dauer eines Monats ausreichend. Soweit diese darüber hinaus für statistische Zwecke benötigt werden, ist ihre Anonymisierung erforderlich.

Die datenschutzrechtliche Verantwortung liegt in erster Linie bei den Verwaltungen als Anbieter nach § 2 Nr. 1 TDDSG bzw. als auftraggebende Stelle nach § 4 Abs. 1 LDSG. Angesichts der Zahl der betroffenen Verwaltungen wurde mit dem LDI als zentralem Auftragnehmer vereinbart, dass die Dauer der Speicherung im bisherigen Umfang zwar beibehalten werden kann, nach Ablauf eines Monats jedoch eine Anonymisierung erfolgt. Die Auftraggeber des LDI wurden über die geänderte Verfahrensweise und die ihr zugrunde liegenden Regelungen unterrichtet.

21.2.6 Verfahren „SecTelMed“ für die Bereitstellung von Radiologiedaten

Für die Bereitstellung von Radiologiedaten an die einzelnen Einrichtungen eines Krankenhauses sowie für Telekonsultationen wurde von einem Klinikum das Verfahren „SecTelMed“ entwickelt. Die radiologischen Informationen werden dabei auf einem vom Klinikum betriebenen Server teilnehmerbezogen bereitgestellt. Für jeden Empfänger existiert ein Verzeichnis, in welches die Radiologiedaten abrufbar eingestellt werden.

Das Verfahren dient derzeit im Wesentlichen als Ersatz für die Weitergabe radiologischer Bilder per Boten. Es ist unabhängig von bestimmten medizinischen Fachanwendungen und benötigt absender-/empfängerseitig lediglich bildgebende oder -verarbeitende Lösungen, die Daten nach dem DICOM-Protokoll (Digital Imaging and Communication in Medicine) verarbeiten können.

Die Radiologiedaten werden für die Übertragung verschlüsselt und digital signiert. Die eingesetzten Softwarekomponenten, Algorithmen und Schlüssellängen sind im Blick auf die Sicherstellung des Datenschutzes nach § 28 Abs. 6 Röntgenverordnung geeignet und begegnen aus Sicht des LfD keinen datenschutzrechtlichen Bedenken. Die genutzte Signaturlösung entspricht dabei einer fortgeschrittenen Signatur nach § 2 Nr. 2 SigG. § 43 Röntgenverordnung sieht die qualifizierte elektronische Signatur für vorgeschriebene Aufzeichnungen, die in elektronischer Form erfolgen, vor. Bei „SecTelMed“ handelt es sich jedoch nicht um ein Verfahren zur Aufzeichnung radiologischer Dokumente, sondern um ein Verfahren zur Übertragung medizinischer Daten. Die im Rahmen von „SecTelMed“ genutzte Signatur dient dabei lediglich der Integritätssicherung während der Datenübertragung. Das Erfordernis einer qualifizierten Signaturlösung gemäß § 2 Nr. 3 SigG besteht damit im vorliegenden Fall nicht.

Die dezentrale Erzeugung der kryptografischen Schlüssel durch die teilnehmenden Stellen war aus Sicht des LfD aufgrund des geschlossenen Benutzerkreises mit überschaubarer Teilnehmerzahl hinnehmbar. Problematisch war hingegen, dass Signaturschlüssel nach Ablauf der Gültigkeitsdauer weiter genutzt werden konnten; eine Überwachung der Gültigkeitsdauer oder eine automatische Sperre abgelaufener Schlüssel erfolgte nicht. Der LfD hat daher empfohlen, das Verfahren entsprechend anzupassen. Bei steigender Teilnehmerzahl bedarf es seiner Ansicht nach allerdings einer tragfähigen Zertifizierung, d. h. der gegenüber Dritten verlässlichen Bestätigung, dass ein Schlüssel einer bestimmten Stelle zugeordnet ist. Die entsprechenden Trustcenter-Aufgaben (Schlüsselerzeugung, Personalisierung, Zertifizierung, Verzeichnisdienst, Gültigkeitsprüfung, Sperrdienst etc.) können – auf der Grundlage vertraglicher Vereinbarungen – Stellen außerhalb des Klinikums wie einer Ärztekammer oder der Deutschen Radiologischen Gesellschaft übertragen werden.

21.2.7 Verfahren „Antrag Online“ der Landesversicherungsanstalt Speyer

Der Verband Deutscher Rentenversicherungsträger (VDR) stellt für die Aufnahme von Leistungsanträgen nach § 151 a SGB VI ein elektronisches Verfahren zur Verfügung. Das Programm ist derzeit bei bundesweit ca. 3 600 Stellen in einer Offline-Version im Einsatz. Die Anträge werden dabei ausgedruckt und auf dem Postweg an die Versicherungsträger verschickt. Künftig soll die Möglichkeit der elektronischen Übermittlung von Rentenanträgen bestehen. Das Gesamtverfahren unterliegt, je nach Art der beteiligten Stellen, unterschiedlichen datenschutzrechtlichen Zuständigkeiten. Die Datenschutzkontrolle des LfD erstreckt sich dabei auf die das Verfahren nutzenden öffentlichen Stellen der rheinland-pfälzischen Landes- und Kommunalverwaltung; der VDR als Spitzenverband der Versicherungsträger auf Bundesebene unterliegt der Kontrolle des BfD.

Im Zusammenhang mit dem Einsatz des Verfahrens bei den Gemeindebehörden und Versicherungsämtern in Rheinland-Pfalz wurde der LfD um Stellungnahme zu dem für das Verfahren erstellte Sicherheitskonzept gebeten. Die Bewertung des Schutzbedarfs, die vorgesehenen Verfahrensweisen und Sicherheitsmaßnahmen sowie die Einschätzung des Restrisikos begegnen dabei aus

seiner Sicht keinen Bedenken. Den Anforderungen aus § 78 a SGB X kann damit in geeigneter Weise entsprochen werden; die nach Umsetzung der vorgesehenen Maßnahmen verbleibenden Restrisiken stehen aus datenschutzrechtlicher Sicht einem Einsatz des Verfahrens nicht entgegen.

Um die angestrebte Verfahrenssicherheit zu erreichen ist eine vollständige Umsetzung des Sicherheitskonzepts erforderlich. Dies gilt vor allem für den durch heterogene IT-Strukturen gekennzeichneten sowie rechtlich und organisatorisch weitgehend selbständigen Bereich der Kommunen. Um die Sicherheit des Gesamtverfahrens zu gewährleisten ist daher vorgesehen, dass die Gemeinden und Versicherungsämter eine Verpflichtungserklärung abgeben, in der die Einhaltung der Leit- und Richtlinien zur Nutzung des Verfahrens, und damit der im Sicherheitskonzept vorgesehenen technisch-organisatorischen Maßnahmen bestätigt wird. Der LfD hat in diesem Zusammenhang empfohlen, in die vom verantwortlichen Ministerium auszusprechende Teilnahmegenehmigung eine entsprechende Auflage aufzunehmen.

21.2.8 Flächeninformationssystem Online Rheinland-Pfalz (FLOrlp)

Das Verfahren FLOrlp ermöglicht in Form einer Web-Anwendung die Online-Abfrage landwirtschaftlicher Förderflächen über das Internet. Hierzu werden aus Geobasisdaten erzeugte digitale Karten über einen Webserver zur Verfügung gestellt. Applikationsserver und Datenserver befinden sich dabei in verschiedenen Sicherheitszonen des rlp-Netzes, die Kommunikation der Systeme erfolgt über die Plattform „rlp-Service24“. Die damit verbundene Auftrennung der Verbindung zwischen den beteiligten Systemen trägt den unterschiedlichen Sicherheitsstufen der Subnetze Rechnung. Im Rahmen der Einführung des Verfahrens ergab sich jedoch die unabweisbare Notwendigkeit, den förderberechtigten Stellen zu einem Zeitpunkt das Verfahren bereitzustellen, zu dem die Plattform „rlp-Service24“ noch nicht im erforderlichen Umfang zur Verfügung stand. Als Konsequenz sollte die Aufteilung der Systeme auf unterschiedliche Sicherheitszonen vorübergehend ausgesetzt werden.

Mit Blick auf die Bedeutung des rlp-Netzes als zentrale Kommunikationsplattform der Landesverwaltung und die in § 1 Abs. 2 LDI-Errichtungsgesetz i. V. m. § 2 Abs. 2 Nr. 3 der Betriebssatzung des LDI genannte Aufgabenstellung befürwortet der LfD eine grundsätzlich restriktive Haltung gegenüber Durchbrechungen der Sicherheitskonzeption des rlp-Netzes. Die Vielzahl der angeschlossenen Stellen und Anwendungen erfordern ein verlässlich einschätzbares Sicherheitsniveau, das im Fall von Ausnahmeregelungen nur eingeschränkt zu gewährleisten ist.

Die für das Verfahren FLOrlp angestrebte Zwischenlösung kam aus Sicht des LfD daher nur übergangsweise als bedarfsbezogene Kommunikation in der Definition der Sicherheitsleitlinien des rlp-Netzes und unter folgenden Voraussetzungen in Betracht:

- Die Anbindung des FLOrlp-Servers wird über eine gefilterte und auf die betroffenen Systeme beschränkte Verbindung unter der administrativen Kontrolle des LDI realisiert.
- Vor Einrichtung der Netzverbindung sind die Konfiguration und Patchlevel der beteiligten Systeme zu überprüfen und gegebenenfalls zu aktualisieren sowie nicht erforderliche Dienste und Anwendungen zu entfernen. Für die verbleibende Konfiguration ist sicherzustellen, dass nachträgliche Sicherheits-Updates zeitnah installiert werden.
- Um eine unzulässige Veränderung von Systemdateien erkennen zu können, sollten vor Einrichtung der Verbindung Prüfsummen der unveränderlichen Teile des Dateisystems angefertigt und diese in angemessenen Abständen überprüft werden.
- Verstöße gegen die Filterregeln der Firewalls am Übergang der jeweiligen Teilnetze sind zu protokollieren und zeitnah zu klären.
- Die Anbindung erfolgt auf der Grundlage einer schriftlichen Beauftragung des LDI und zeitlich begrenzt. Sobald die Plattform „rlp-Service24“ zur Verfügung steht, ist das Verfahren umzustellen.

Der Landesbeauftragte hat ergänzend darauf hingewiesen, dass es sich bei der dargestellten Verfahrensweise um eine angesichts der nachteiligen Folgen eines verzögerten Verfahrensbeginns mitgetragene Ausnahmeregelung ohne Modellcharakter handelt. Den Empfehlungen des LfD wurde entsprochen.

21.2.9 Anbindung rheinland-pfälzischer Stellen an die Dialoganwendungen des Kraftfahrtbundesamtes (KBA)

Die Anbindung der die Dialoganwendungen des KBA nutzenden Stellen in Rheinland-Pfalz erfolgt über eine eigene Festverbindung des LDI. Diese besteht seit mehreren Jahren und soll nunmehr in einen Zugang über das TESTA-Netz überführt werden. Für dieses betreibt der LDI einen firewallgesicherten Zugang, der unter kontrollierten Bedingungen von den zugelassenen Stellen der Landes- und Kommunalverwaltung erreichbar ist. Ausgehend von den bestehenden Sicherheitsstrukturen hat der LDI ein Konzept erarbeitet, mit dem ein gesicherter Zugang zu den KBA-Anwendungen gewährleistet werden soll. Im Zusammenhang mit der Umstellung wurde der LfD um Stellungnahme zu der vom LDI geplanten Lösung gebeten.

Im Gegensatz zur Situation in einigen anderen Bundesländern sind die auf das KBA-Portal zugreifenden Stellen in Rheinland-Pfalz nicht über ISDN-Zugänge angebunden. Deren Zugriff erfolgt vielmehr über das vom Landesbetrieb Daten und Information administrierte rlp-Netz der Landesverwaltung bzw. das Kommunale Netz Rheinland-Pfalz (KNRP). Beide sind aufgrund ihrer technischen Gestaltung und die Art des Netzmanagements (vgl. Tz. 21.2.2 und 21.2.3) als sichere und geschlossene Netze i. S. d. § 13 Abs. 1 Satz 3 FRV bzw. § 54 Abs. 1 Satz 3 FeV anzusehen.

Trotz einer damit grundsätzlich möglichen Verwendung einer netzweit einheitlichen Zugangskennung wurden für die abrufenden Stellen in Rheinland-Pfalz dienststellenbezogene Kennungen vergeben. In Verbindung mit der Zuordenbarkeit der Netz-Adressen zu bestimmten Verwaltungen ergibt sich damit eine angemessene Authentizität und Nachvollziehbarkeit der abrufenden Stellen. Der nutzenden Verwaltung obliegt es dabei sicherzustellen, dass die abrufende natürliche Person festgestellt werden kann (§ 54 Abs. 1 Satz 5 FeV, § 13 Abs. 1 Satz 5 FRV).

Darüber hinaus ist im Konzept des LDI vorgesehen, die IP-Adresse der Endgeräte in die Verbindungs- und Dienstekontrolle des LDI einzubinden und damit eine angemessene Authentizität des Endgeräts beim Zugriff auf das KBA-Portal zu gewährleisten.

Sowohl im rlp-Netz als auch im Kommunalnetz werden die Verbindungen zwischen der jeweils angeschlossenen Verwaltung und dem LDI kryptografisch abgesichert. Dies erfolgt über separate Verschlüsselungsgeräte an den Endpunkten einer Verbindung; deren Management liegt ausnahmslos in der Hand des LDI. Die genutzten Verfahren entsprechen dem Stand der Technik. Angesichts der ebenfalls verschlüsselten Kommunikation im TESTA-Netz ergibt sich damit auf Netzebene eine gesicherte Verbindung von der abrufenden Stelle bis zum KBA-Portal. Der in § 30 a Abs. 2 Nr. 1 StVG geforderten Vertraulichkeit und Unversehrtheit der Datenübertragung wird damit entsprochen.

Die technischen und administrativen Gegebenheiten im rlp-Netz bzw. im Kommunalen Netz gewährleisten aus Sicht des LfD eine Vertraulichkeit der Kommunikation und Authentizität der nutzenden Stellen, die den gesetzlichen Vorgaben für die KBA-Register entsprechen. Angesichts der vertrauenswürdigen IT-Strukturen in den Verwaltungsnetzen des Landes begegnete das Konzept des LDI daher keinen datenschutzrechtlichen Bedenken.

21.2.10 Verfahren zur EDV-gestützten Dokumentation und Analyse sozialer Arbeit von AIDS-Hilfen (DoSA)

Für die Leistungs- und Tätigkeitsdokumentation im Bereich der AIDS-Hilfe wird über das MASFG das Verfahren „DoSA“ zur Verfügung gestellt. Im Rahmen einer Stellungnahme zum Verfahrenskonzept hatte der LfD in einzelnen Bereichen Änderungen bzw. Ergänzungen empfohlen, die bei der weiteren Entwicklung des Programms berücksichtigt werden sollten.

So verfügte das Verfahren über Funktionen zur Benutzerverwaltung und Zugriffskontrolle, die die Möglichkeit boten, verschiedene Benutzer mit je nach Aufgabenstellung unterschiedlich ausgeprägten Zugriffsrechten einzurichten. Dies erlaubte es grundsätzlich, den Datenzugriff angemessen zu beschränken; insgesamt bestand allerdings das Risiko, dass unzureichende Passworte verwendet wurden. Um einen wirksamen Schutz der Anwendung zu gewährleisten, hat der LfD empfohlen, für standardmäßig vergebene Passworte bei der ersten Anmeldung zwingend eine Änderung vorzusehen und Passworte auf die bestehenden Vorgaben hin zu überprüfen.

Der zur Absicherung gespeicherter Daten vorhandene Kennwortschutz reichte lediglich als Schutz vor zufälligem oder unabsichtlichem Zugriff aus und widerstand weitergehenden Zugriffsversuchen nur bedingt. So war es im Rahmen von Tests möglich, die Struktur der Tabellen und Teile des Datenbankkennworts auszulesen. Um eine verlässliche Absicherung zu erreichen, hat der LfD empfohlen, vorhandene Überlegungen zum Einsatz ergänzender Verschlüsselung umzusetzen, zumal die ins Auge gefasste Lösung auch zugleich eine angemessene Vertraulichkeit gegenüber Personen gewährleistet, die über weitgehende Zugriffsmöglichkeiten auf das jeweilige System verfügen, ohne im Rahmen der eigentlichen AIDS-Hilfe tätig zu werden (z. B. Systembetreuung, Wartungsunternehmen).

Mit Blick auf die Sensibilität der in DoSA gespeicherten Daten sollte weiterhin gewährleistet werden, dass der Aufruf von Programmfunktionen, die zur Anzeige personenbezogener Daten führen, mit der Angabe über den jeweiligen Benutzer und des Zeitpunkts des Aufrufs manipulationsfest protokolliert werden.

21.2.11 Schulintranet in einem Landkreis

Ein Landkreis hat gemeinsam mit einem lokalen Internetserviceprovider und IT-Dienstleister den Aufbau eines Schulintranets für die in Trägerschaft des Landkreises stehenden Schulen geplant und bereits teilweise realisiert. Der LfD wurde frühzeitig einbezogen. Im März 2003 wurde bei einer gemeinsamen Besprechung mit Vertretern der Kreisverwaltung und dem Dienstleister als Projektpartner das Konzept konkret erläutert. Forderungen, die sich aus datenschutzrechtlicher Sicht ergeben haben, konnten somit bereits vor Erstellung eines Leistungsverzeichnisses (als Grundlage für eine spätere Ausschreibung) berücksichtigt werden.

Während des gesamten Projektablaufes wurde der LfD regelmäßig über den aktuellen Projektstand informiert.

Aus datenschutzrechtlicher Sicht waren folgende Punkte besonders zu berücksichtigen:

a) Beibehaltung der Trennung von Unterrichtsnetzen und Schulverwaltungsnetzen

   Das geplante Schulintranetprojekt bezieht sich lediglich auf die Unterrichtsnetze. Eine Koppelung mit den Schulverwaltungsnetzen ist nicht vorgesehen. Diese ausdrückliche Empfehlung des LfD wurde von Beginn an unterstützt. Somit ist sichergestellt, dass die sensiblen Daten der Schulverwaltung nicht einem möglichen „Angriff“ seitens der Unterrichtsnetze ausgesetzt sind.

b) Technische und organisatorische Maßnahmen zur Sicherung der Komponenten

Durch die frühe Beteiligung des LfD konnten Anforderungen an die IT-Sicherheit bereits in die Erstellung der Leistungsverzeichnisse einfließen. Hier sind insbesondere die Sicherstellung einer vertraulichen Kommunikation auf den Funkstrecken durch den Einsatz von kryptografischen Verfahren, die Absicherung der zentralen IT-Komponenten durch Firewalls und der Einsatz von Virenscannern zur Erkennung und Filterung von Schadsoftware zu nennen. Es wurden u. a. Empfehlungen aus dem Kreis der Datenschutzbeauftragten sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) berücksichtigt.

Wesentliche organisatorische Punkte betreffen die beim Betrieb der zentralen Komponenten entstehenden Protokolldaten. Die Logdateien der Server beinhalten personenbezogene bzw. personenbeziehbare Daten, die Rückschlüsse auf das Nutzungsverhalten der zugangsberechtigten Personen zulassen. Dass diese Protokollinformationen – die für den ordnungsgemäßen Betrieb zweifellos erforderlich sind – nicht außerhalb des rechtlich zulässigen Bereichs ausgewertet werden, wird Gegenstand von Nutzungsbestimmungen für das Schulintranet sein. Erkenntnisse, die im Rahmen der Pilotphase gewonnen werden, können als Maßstab für weitere Projektphasen dienen.

c) Das Verhältnis zwischen Schulträger und Dienstleister: Datenverarbeitung im Auftrag

Der Betrieb der Schulnetze ist originäre Aufgabe der Kreisverwaltung als Schulträger. Da sie den Betrieb durch einen privaten Dienstleister vornehmen lässt, entsteht ein Auftragsdatenverhältnis im Sinne des Landesdatenschutzgesetzes. Dies ist bei der Vertragsgestaltung zu berücksichtigen, insbesondere im Hinblick auf Weisungs- und Kontrollbefugnisse. Die beteiligten Stellen wurden bereits in den Vorbesprechungen auf diese Punkte hingewiesen.

Wie die Kreisverwaltung zwischenzeitlich mitgeteilt hat, ist in den Verträgen den Anforderungen des § 4 LDSG Rechnung getragen worden. Gleichzeitig mit der Vertragsunterzeichnung wurden die am Projekt beteiligten Mitarbeiter des Dienstleisters auf das Landesdatenschutzgesetz sowie nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) verpflichtet.

21.3 Allgemeine technisch-organisatorische Aspekte

21.3.1 Automatisierte Weiterleitung dienstlicher E-Mails zu privaten Postfächern

Im Rahmen des Einsatzes von E-Mail-Lösungen wurde die Frage an den LfD herangetragen, inwieweit eine automatisierte Weiterleitung dienstlicher E-Mails zu privaten Postfächern möglich ist.

Die Möglichkeit, eingehende E-Mails automatisiert an ein anderes Mail-Konto weiterzuleiten, ist fraglos mit erheblichem Nutzen verbunden. So erlaubt sie es insbesondere, für Abwesenheitsfälle geeignete Vertretungsregelungen abzubilden oder weitere beteiligte Stellen unmittelbar zu unterrichten. Sie dient damit dem Anliegen der Verwaltungen, auch für die E-Mail-Kommunikation einen raschen und ordnungsgemäßen behördlichen Geschäftsgang zu gewährleisten. Innerhalb der jeweiligen Verwaltung und bei Beachtung der Anforderungen des § 9 Abs. 2 Nr. 3 LDSG ist sie daher unproblematisch.

Die Verarbeitung dienstlicher Daten im privaten Umfeld kann in diesem Zusammenhang jedoch nur eine Ausnahme darstellen. Die Fälle, in welchen dies regelmäßig erfolgt, etwa bei Tele- oder Heimarbeitslösungen, unterliegen besonderen organisatorischen und technischen Regelungen, mit denen ein der Büroumgebung des Dienstherrn vergleichbares Schutzniveau gewährleistet werden soll.

Anders ist die Weiterleitung dienstlicher Mails an private E-Mail-Adressen von Bediensteten zu bewerten. Hier ist aus Sicht des LfD zweifelhaft, ob der nach § 9 Abs. 2 Nr. 4 LDSG geforderte Schutz vor unbefugter Kenntnisnahme verlässlich sichergestellt werden kann. Unabhängig von der Frage einer vertraulichen Übertragung sind die Art privater Maillösungen und die dabei bestehenden Zugriffsmöglichkeiten höchst unterschiedlich und entziehen sich in aller Regel der Beurteilung und Einflussnahme des Dienstherrn.

Für Nachrichten ohne Personenbezug ist die Weiterleitung aus datenschutzrechtlicher Sicht naturgemäß unbedenklich. Auch mag für herausgehobene Funktionen eine Weiterleitung von Mails mit personenbezogenem Inhalt fallweise erforderlich sein; die überschaubare Zahl dieser Fälle erlaubt es jedoch, angemessene Schutzvorkehrungen gegen eine unbefugte Kenntnisnahme zu treffen. Eine allgemeine und pauschale Weiterleitung dienstlicher Mails auf private Mail-Konten lediglich mit dem Ziel, abends, am Wochenende oder während des Urlaubs die Einsichtnahme zu eröffnen, begegnet jedoch datenschutzrechtlichen Bedenken.

Die Hinweise der anfragenden Verwaltung sahen zwar vor, dass eine Weiterleitung nur eingerichtet werden darf, wenn nicht mit dem Eingang personenbezogener oder anderweitig schützenswerter Daten gerechnet wird, es bestehen aus Sicht des LfD jedoch Zweifel, ob bei einer routinemäßigen Nutzung der Weiterleitungsfunktion in der Praxis eine entsprechende Abschätzung und Differenzierung möglich ist. In manchen Bereichen mag dies der Fall sein und dort steht einer Weiterleitung aus datenschutzrechtlicher Sicht nichts entgegen. Häufig ist jedoch nicht verlässlich absehbar, welcher Art eingehende E-Mails sind. Der LfD hält es für sinnvoll, den Ausnahmecharakter der Weiterleitung und den Rückgriff auf bestehende Vertretungsregelungen zu betonen.

Der LfD hat empfohlen, in die Dienstanweisungen zur Nutzung von E-Mail-Lösungen folgende Hinweise aufzunehmen:

- Eine pauschale Weiterleitung dienstlicher E-Mails auf private Mailkonten von Bediensteten ist grundsätzlich nicht zugelassen; Ausnahmen bedürfen der Genehmigung der Behördenleitung. Eingehende Nachrichten sind bei Abwesenheit zunächst entsprechend der bestehenden Vertretungsregelungen weiterzuleiten.
- Die Weiterleitung dienstlicher Mails zu privaten Mailadressen ist nur im Einzelfall zulässig und nur, wenn dies aus sachlichen und zeitlichen Gründen zwingend geboten ist. Dabei dürfen keine schützenswerten personenbezogenen Daten oder im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen (Verschlusssachen) betroffen sein.
- Die genutzten privaten Mailkonten dürfen dabei nur im Zugriff von Mitarbeitern der Verwaltung stehen; ein Zugriff weiterer Nutzer (z. B. von Familienmitgliedern) muss ausgeschlossen sein.
- Die weitergeleiteten dienstlichen Nachrichten sind, wenn ihre Speicherung nicht mehr erforderlich ist, unverzüglich zu löschen.

21.3.2 Filterung von E-Mail-Anhängen im Rahmen des Virenschutzes

Der LfD wurde im Berichtszeitraum mehrfach um Beratung zu datenschutzrechtlichen Fragen bei der Verarbeitung von E-Mails im Zusammenhang mit Maßnahmen zum Schutz vor Computerviren gebeten.

Mit Blick auf die Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage sind Maßnahmen zur Filterung von E-Mails mit potentiell sicherheitskritischem Inhalt – wie z. B. Computerviren – aus datenschutzrechtlicher Sicht grundsätzlich nicht zu beanstanden; sie unterfallen dem Bereich der Weitergabe- bzw. Verfügbarkeitskontrolle nach § 9 Abs. 2 Nr. 4 und 7 LDSG.

Die Entscheidung, welche Maßnahmen konkret getroffen werden, etwa, ob bestimmte Dateianhänge grundsätzlich unterdrückt werden, liegt zunächst in der Organisationshoheit der jeweiligen Stelle. Datenschutzrechtlich vertretbare Lösungen bestehen z. B. darin, dass entsprechende Inhalte ausgefiltert werden, und ein Hinweis an den Empfänger der Mail ergeht. Eine Zustellverpflichtung für jegliche Mailinhalte lässt sich, zumal für den Bereich der dienstlichen Nutzung, datenschutzrechtlich nicht begründen. Soweit der Empfänger nicht innerhalb eines festgelegten Zeitraums die weitere Behandlung der Nachricht mit der für den IT-Einsatz verantwortlichen Stelle abstimmt, kann diese automatisiert gelöscht werden. Um die notwendige Transparenz für die Nutzer sicherzustellen, sollten die entsprechenden Regelungen in einer Dienstanweisung dokumentiert werden (vgl. hierzu auch die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter www.datenschutz.rlp.de).

Die vorstehenden Gesichtspunkte betreffen zunächst den Bereich der dienstlichen Nutzung. Soweit der Arbeitgeber eine private Nutzung zulässt (vgl. hierzu auch Tz. 19.3), ist es ihm grundsätzlich möglich, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Voraussetzungen nicht erfüllen wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

21.3.3 Absicherung von Funknetzen (WLAN)

Unter dem Begriff WLAN – Wireless Local Area Network – hat die Rechner-Vernetzung per Funk zunehmend Bedeutung erlangt. Aktuelle Systeme sind häufig bereits werkseitig entsprechend ausgestattet; dies ermöglicht es, sich ad hoc in vorhandene Funknetze einzuklinken.

So komfortabel dies im Einzelfall ist, ergeben sich daraus jedoch auch Sicherheitsrisiken. Anders als bei kabelgebundenen Netzen sind aufgrund der Nutzung von Funkwellen Angriffe möglich, auch ohne dass ein direkter räumlicher Zugang besteht. Soweit Funknetze vertraulich betrieben werden sollen, bedürfen sie daher einer geeigneten Absicherung. Aufgrund des Hinweises eines Bürgers auf vermutete offen zugängliche Netze im Bereich der Landesregierung hat der LfD entsprechende Kontrollen durchgeführt. Diese betrafen Funknetze im Regierungsviertel und an weiteren ausgewählten Orten mit Landesbehörden bzw. Regierungsstellen in Mainz.

Insgesamt konnten dabei 290 Funknetze lokalisiert werden, wovon ca. 5 % ohne jeglichen Schutz offen zugänglich waren. Es ergaben sich jedoch keine Hinweise darauf, dass diese Netze dem behördlichen Bereich zuzuordnen waren. Den verwendeten Netzkennungen und der Art der eingesetzten Komponenten nach handelte es sich aller Wahrscheinlichkeit nach um privat betriebene Netze.

Bei mehr als der Hälfte der vorgefundenen Netze (56 %) wurde der Datenverkehr nicht verschlüsselt; mit Hilfe frei verfügbarer Programme war hier eine Aufzeichnung der Kommunikation möglich. Bei den im verschlüsselten Modus betriebenen Funknetzen kam in 95 % der Fälle mit dem WEP-Verfahren (Wireless Equivalence Privacy) ein vergleichsweise schwacher Schutzmechanismus zum Einsatz.

Zur Klärung, welchen Aufwand potentielle Angreifer treiben müssten, um diese Form der Verschlüsselung zu brechen, wurde unter nachgestellten Bedingungen vom LfD ein Angriff auf ein solcherart geschütztes Funknetz durchgeführt. Dabei wurden ca. zwei Personentage für die Beschaffung, Installation und Konfiguration der notwendigen Programme sowie für den Aufbau der erforder-

lichen Fachkenntnis benötigt. Nach einem Mitschnitt des Netzverkehrs von ca. 35 Minuten war die notwendige Anzahl geeigneter Datenpakete für einen Angriff vorhanden. Die Verschlüsselung konnte auf handelsüblichen Rechnern anschließend nach zehn bis 15 Sekunden gebrochen werden. Unter Praxisbedingungen dürfte der Zeitaufwand für eine erfolgreiche Entschlüsselung nach Einschätzung des LfD etwas höher liegen, da hier in der Regel nicht die volle Bandbreite des Funknetzes ausgenutzt wird. Nach den Erfahrungen des LfD stellen die in der Literatur genannten drei bis fünf Stunden jedoch einen realistischen Zeitraum dar.

Eine Absicherung von Funknetzen allein auf Basis der WEP-Verschlüsselung ist damit aus Sicht des LfD unzureichend. Da für den überwiegenden Teil der vorgefundenen Funknetze diese Verschlüsselungsform zum Einsatz kam, hat er die Ressorts angeschrieben und empfohlen, den Einsatz und Betrieb etwaiger Funknetze zu überprüfen und Sicherheitsmaßnahmen gegebenenfalls neu zu bewerten bzw. anzupassen. Hinweise hierzu finden sich in der Orientierungshilfe „Datenschutz in drahtlosen Netzen“ des Arbeitskreises Technik der Datenschutzbeauftragten (www.datenschutz.rlp.de).

21.3.4 Zugriffskontrolle bei Internet-Angeboten

Im Rahmen der Online-Kontrolle eines Internet-Angebots wurde vom LfD Rheinland-Pfalz überprüft, ob und gegebenenfalls welche Zugriffsmöglichkeiten auf die Protokolldaten bestanden, durch die das Nutzerverhalten erfasst wurde. Die verantwortliche öffentliche Stelle bediente sich dabei für den Betrieb des Webservers der von einer Bundesbehörde bereitgestellten Mechanismen und IT-Strukturen.

Bei der Kontrolle hat sich ergeben, dass die auf dem Server eines Dienstleisters der Bundesbehörde gespeicherten Zugriffsdaten allgemein zugänglich waren und über das Internet abgerufen werden konnten. Die Daten ließen u. a. erkennen, zu welchem Zeitpunkt und unter welcher Rechner-Adresse (IP-Adresse) auf bestimmte Internet-Angebote zugegriffen wurde. Nach dem gegenwärtigen Kenntnisstand wurde es bei einer technischen Umstellung versäumt, die bis dahin betriebenen Verfahren anzupassen und vorhandene Datenbestände und Zugriffsmöglichkeiten zu bereinigen.

Für den administrativen Bereich des betroffenen Internet-Servers war der Zugriff passwortgesichert; bestimmte Angaben in den frei im Zugriff stehenden Seiten erlaubten jedoch den Rückschluss auf die verwendeten Benutzerkennungen.

Eine daraufhin durchgeführte automatisierte Attacke auf den Passwortschutz wurde nach ca. 600 000 Versuchen abgebrochen. Hintergrund war, dass im Fall einer Protokollierung der unzulässigen Zugriffsversuche ein Datenvolumen erzeugt worden wäre, durch das die Verfügbarkeit des Webservers hätte beeinträchtigt werden können. Die bis dahin vorgenommenen Versuche hatten bereits zu einem Protokollvolumen von 500 Megabyte geführt. Die im Nachgang erfolgte Klärung hat ergeben, dass der Angriff seitens des Serverbetreibers trotz Protokollierung nicht registriert wurde.

Der LfD hat unmittelbar nach den Feststellungen das zuständige Ministerium unterrichtet. Die bemängelten Zugriffsmöglichkeiten wurden daraufhin unterbunden. Ergänzend soll eine Auditierung des Verfahrens durch das Bundesamt für Sicherheit in der Informationstechnik in Auftrag gegeben werden.

Da in der Angelegenheit auch eine Bundesbehörde betroffen war, hat der LfD den Bundesbeauftragten für den Datenschutz unterrichtet.

21.4 Datenschutzregister/Verfahrensverzeichnis

Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, sind von der verantwortlichen Stelle beim LfD zur Eintragung in das dort geführte Datenschutzregister anzumelden (§ 27 Abs. 1 LDSG). Für den LfD bilden diese Eintragungen eine wichtige Grundlage der Kontrollarbeit. Auch die behördlichen Datenschutzbeauftragten können aus den Anmeldungen die Informationen entnehmen, die sie für die Wahrnehmung ihrer Aufgaben nach § 11 LDSG benötigen.

Häufig werden grundsätzliche datenschutzrechtliche Defizite, wie z. B. das Fehlen von Löschungsfristen oder Speicherungen nicht erforderlicher personenbezogener Merkmale in automatisierten Verfahren nur aufgrund von Anmeldungen zum Datenschutzregister bekannt. Darüber hinaus gab es in der Vergangenheit aufgrund der Anmeldungen häufig Veranlassung, örtliche Feststellungen durchzuführen und datenschutzrechtliche Verbesserungen anzuregen.

Die Bedeutung des Datenschutzregisters für die Datenschutzkontrolle wird auch aus der zahlenmäßigen Entwicklung der Anmeldungen erkennbar. Im Jahre 1986 wurde das Datenschutzregister auf eine automatisierte PC-Anwendung umgestellt. Damals waren im Datenschutzregister ca. 3 200 Anwendungen gespeichert, heute sind es bereits über 9 200.

Der LfD ist bemüht, den mit dem Anmeldeverfahren verbundenen Verwaltungsaufwand so gering wie möglich zu halten. Daher ist geplant, künftig eine Möglichkeit zu schaffen, dass verantwortliche Stellen ihre Anmeldungen auch online über ein vom LfD bereitgestelltes Formular vornehmen können. Darüber hinaus wird von einigen Ressorts über den Aufbau eines zentralen Verfahrensverzeichnisses nachgedacht. Eine Vorreiterrolle spielt dabei die rheinland-pfälzische Polizei, die gemeinsam mit dem LfD ein zentrales Verfahrensverzeichnis der Polizei entwickelt hat. Damit ist es möglich, Anmeldungen nur einmal zu erfassen und die Informationen über ein spezielles Rollenkonzept allen zuständigen Stellen einschließlich dem LfD im Rahmen ihrer Zuständigkeit zur Verfügung zu stellen. Eine entsprechende Pilotanwendung befindet sich derzeit in der Erprobung.

22. Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen

22.1 Eine Sparkasse und ihr Selbstverständnis von Datenschutz

Ein Petent begehrte bei einer Sparkasse Einsicht in dort über ihn vorgehaltene personenbezogene Daten. Als ihm die Auskunft nicht im gewünschten Umfang erteilt wurde, bat er den LfD um Hilfe. Die Sparkasse, wie in solchen Fällen üblich, wurde um eine Stellungnahme zu dieser Angelegenheit gebeten. Sie teilte jedoch lediglich mit, dass sie die Kontrollkompetenz des LfD nicht für gegeben halte, da der Anwendungsbereich des Bundesdatenschutzgesetzes nicht eröffnet sei.

Diese Auffassung wurde nicht geteilt: Der Umfang der Kontrollaufgaben des LfD gegenüber öffentlich-rechtlichen Kreditinstituten bestimmt sich gem. §§ 2 Abs. 4 LDSG, 38 BDSG. Danach kontrolliert der LfD die Ausführung des BDSG sowie anderer Vorschriften über Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Es gehört danach auch zu seinen Aufgaben, zu überprüfen, ob Betroffene gem. § 34 BDSG einen Auskunftsanspruch haben und ob die Auskunft von den seiner Kontrolle unterliegenden Stellen erteilt wurde. Dazu muss er über die Informationen verfügen, die eine Überprüfung des Vorliegens der Tatbestandsvoraussetzungen ermöglichen. Folglich musste er im vorliegenden Fall wissen, ob und in welcher Form Daten über den Petenten vorliegen. Sodann konnte er beurteilen, ob die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben wurden oder ob sie in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben wurden und damit der Anwendungsbereich des BDSG eröffnet war. Weiterhin benötigte er Informationen für die Feststellung, ob eine Pflicht zur Auskunftserteilung gem. § 34 Abs. 4 BDSG evtl. nicht bestand. Entsprechende Anhaltspunkte, wonach der Anwendungsbereich des BDSG nicht eröffnet war oder ein Auskunftsanspruch gar nicht bestand, hatte die Sparkasse aber nicht vorgetragen. Sie hatte lediglich ohne weitere Begründung festgestellt, dass die fraglichen Daten weder automatisiert verarbeitet noch in oder aus automatisierten Dateien verarbeitet würden. Der LfD wies in diesem Zusammenhang darauf hin, dass auch diese Beurteilung seiner Kontrollkompetenz unterliegt. Andernfalls könnte sich die Sparkasse mit einer entsprechenden Schutzbehauptung jeglicher datenschutzrechtlicher Kontrolle entziehen.

Um die Angelegenheit weiter zu überprüfen und die fraglichen Unterlagen in Augenschein nehmen zu können, kündigte der LfD seinen Besuch bei der Sparkasse an. Ein Betreten der Räumlichkeiten wollte diese jedoch nur ohne Anerkennung eines Rechtsanspruchs unter für den LfD nicht akzeptablen Bedingungen gestatten. Erst nach Einschaltung des FM als Aufsichtsbehörde für die Sparkassen konnte ein sachliches Gespräch zwischen Sparkasse und LfD geführt werden, bei dem auch die Art der fraglichen Datenverarbeitung geprüft werden konnte. Die Einordnung der Unterlagen erwies sich als schwierig. Eine automatisierte Datenverarbeitung lag nicht vor. Fraglich war daher, ob es sich um eine nicht automatisierte Datei handelte. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann (§ 3 Abs. 2 Satz 2 BDSG). Bei der Kundenakte, in der die Informationen über den Petenten enthalten waren, handelte es sich jedoch nicht um eine solche nicht automatisierte Datei. Es lag zwar eine Sammlung in Form einer Kundenakte vor, diese war jedoch nicht gleichartig aufgebaut. Das BDSG schützt aber gerade nicht jede Sammlung personenbezogener Daten z. B. in Akten, sondern nur solche, bei denen die Form der Aufbewahrung zur leichten und damit möglicherweise auch missbräuchlichen Auswertung führen kann. Dies war hier nicht der Fall. Ein Anspruch auf Auskunft konnte daher nicht auf § 34 BDSG gestützt werden.

Aufgrund der mangelnden Kooperation der Sparkasse konnte die Angelegenheit für keinen der Beteiligten so schnell erledigt werden, wie es datenschutzrechtlich wünschenswert gewesen wäre.

22.2 Auswertung von Girokontodaten

Eine Sparkasse beabsichtigte, Daten von Girokontobewegungen in personenbezogener Form auszuwerten. So sollte z. B. überprüft werden, welche Kunden monatlich eine Miete in bestimmter Höhe überweisen. Diesen sollte sodann ein Angebot zur Immobilienfinanzierung unterbreitet werden. Die Sparkasse hielt ein solches Vorgehen für zulässig, da die Kunden bei Eröffnung des Girokontos ankreuzen konnten, ob sie mit Telefonwerbung einverstanden sind und zudem nach Erhalt eines Werbebriefes solchen Maßnahmen zukünftig widersprechen konnten. Das Einverständnis bzw. der nicht vorgenommene Widerspruch seien ausreichende Grundlage für die Datenauswertung.

Die Verarbeitung und Nutzung personenbezogener Daten ist gem. § 4 Abs. 1 BDSG nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

Fraglich war, ob die Erklärung, man sei mit Telefonberatung und -werbung einverstanden, eine ausreichende Einwilligung in die Datenauswertung darstellte. Die Einwilligung ist gem. § 4 a Abs. 1 BDSG nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Diese Voraussetzungen waren hier nicht erfüllt: Aus dem Stichwort „Einverständnis mit Telefonberatung und -werbung“ ergab sich für den Betroffenen nicht, dass hierzu zuvor die Daten seines Girokontos ausgewertet wurden. Denn Werbeaktionen können auch „blind“ erfolgen, ohne dass zuvor ein bestimmter Kundenkreis ausgewählt wurde. Die Einwilligungserklärung hätte zumindest um den Hinweis ergänzt werden müssen, dass zu diesem Zweck auch die Kontobewegungen ausgewertet werden. Nur ein solcher Hin-

weis konnte Grundlage einer informierten Einwilligung sein. Die vorliegende Erklärung war hierzu nicht bestimmt genug. Dabei war auch zu bedenken, dass es sich bei den Informationen um teilweise sehr sensitive Daten handeln konnte, wenn z. B. Beiträge an Parteien oder Religionsgemeinschaften gezahlt wurden. Aus der Gesamtheit der Daten könnte sehr schnell ein Profil des Kunden erstellt werden, da die Teilnahme am Wirtschaftsleben heute fast vollständig über Girokonten läuft. Daher sind gerade Kreditinstitute besonders verpflichtet, die Daten vertraulich zu behandeln und nur im erforderlichen Umfang zu bearbeiten.

Weiterhin kam eine Datenauswertung nach § 28 Abs. 1 Nr. 1 BDSG in Betracht. Danach ist die Datennutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Aus dem vorliegenden Mustervertrag ergab sich nicht, dass über die Abwicklung des Zahlungsverkehrs hinaus weitere Leistungen wie die Werbung oder Beratung nach vorangegangener Datenauswertung vereinbart waren. Aus einem Girovertrag und auch einer längeren entsprechenden Geschäftsbeziehung ergibt sich noch kein Rahmenvertrag, der als Grundlage für eine umfassende Werbung und Beratung herangezogen werden könnte. Ein solcher Rahmenvertrag wird dem Vertragsbegriff nicht gerecht, da es an einer eigenständigen bindenden Rechtsfolge fehlt, die durch die Willenserklärungen der Parteien in Kraft gesetzt wird (BGH NJW 2002, 3695). Folglich diente die Datenauswertung nicht der Erfüllung des Girovertragsverhältnisses. Dies wäre nur dann anzunehmen gewesen, wenn z. B. eine Überweisung falsch ausgeführt wurde und das Kreditinstitut diesen Fehler aufklären wollte. Ein Rückgriff auf Kontendaten hielte sich dann im Rahmen der Vertragsabwicklung und wäre damit zulässig gewesen. Eine Datenauswertung im geplanten Sinn gem. § 28 Abs. 1 Nr. 1 BDSG war danach unzulässig.

Eine Datennutzung kommt schließlich gem. § 28 Abs. 1 Nr. 2 BDSG in Betracht, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Es gehört sicherlich zu den berechtigten Interessen eines Kreditinstituts, durch gezielte Werbemaßnahmen die Geschäftsbeziehungen mit Kunden zu erweitern. Jedoch überwog hier das Interesse der Kunden am Ausschluss der Nutzung. Wie bereits oben dargestellt, wurden hier teilweise sehr sensitive Daten verarbeitet, aus denen auch Kundenprofile erstellt werden konnten. Kreditinstitut und Kunde haben daher ein besonders vertrauenswürdiges Verhältnis. Dies findet auch im sog. Bankgeheimnis seinen Niederschlag, das von den Kreditinstituten stets zu beachten ist. Die auf den Werbeschreiben vorgesehene Widerspruchsmöglichkeit verhinderte nur, dass zukünftige Auswertungen und Werbeaktionen unterbleiben, stellte aber keine Grundlage für die bereits erfolgte Auswertung dar. Eine Datennutzung auf Grundlage von § 28 Abs. 1 Nr. 2 BDSG schied daher ebenfalls aus.

Folglich war die Auswertung von Girokontodaten, soweit sie nicht auf einer ausreichend informierten Einwilligung der Betroffenen beruhte, unzulässig. Diese Auffassung wird auch von den Aufsichtsbehörden für den privaten Bereich vertreten (vgl. LfD NRW 16. Tb. 2003, Ziff. 8.5.1; Innenministerium B-W Tb. 2003, Ziff. 7.6). Da dieses Thema für alle Sparkassen relevant sein dürfte, wurde auch der Sparkassen- und Giroverband über das Ergebnis der Prüfung unterrichtet.

22.3 Bei Anruf Werbung

Der Kunde einer Sparkasse fand auf seinem Kontoauszug den Hinweis, dass er zukünftig interessante Angebote per Telefon erhalten werde, wenn er dem nicht ausdrücklich und schriftlich widerspreche. In diesem Zusammenhang wies der LfD die Sparkasse auf Folgendes hin:

Grundsätzlich dürfen Sparkassen gem. § 28 Abs. 3 Nr. 3 BDSG Kundendaten für Zwecke der Werbung unter bestimmten Voraussetzungen nutzen. Der Betroffene hat gem. § 28 Abs. 4 BDSG das Recht, dieser Datennutzung für Werbezwecke zu widersprechen. Dann ist eine entsprechende Nutzung unzulässig.

Nach ständiger Rechtsprechung des BGH setzt Telefonwerbung jedoch die ausdrückliche Einwilligung der Betroffenen voraus. Das Einverständnis darf nicht mittels einer Formularklausel in den allgemeinen Geschäftsbedingungen abverlangt werden. Nach Auffassung des BGH beeinträchtigt Telefonwerbung die Privatsphäre besonders schwerwiegend. Sie dringe praktisch unkontrollierbar in die Lebensgewohnheiten des Angerufenen ein und zwinge ihm – zu Zeitpunkten, die ausschließlich der Werbende bestimme – Anpreisungen von Waren und Dienstleistungen in seinem häuslichen Bereich auf. Diese massive Einflussnahme, der sich der Adressat häufig nur durch die Verletzung aller Regeln der Höflichkeit entziehen könne, missbrauche den Telefonanschluss, den der Anschlussinhaber im eigenen Interesse und auf eigene Kosten unterhalte, zu Werbezwecken (vgl. Urteil des BGH vom 16. März 1999 – XI ZR 76/98). Wenn Kunden daher nicht ausdrücklich in die telefonische Werbung eingewilligt hatten, was hier offensichtlich der Fall war, war das Vorgehen der Sparkasse unzulässig.

Die Sparkasse erklärte, man habe mit dem fraglichen Verfahren nur das Interesse der Kunden an einem solchen Service abfragen wollen. Unter dem Eindruck der Beschwerde habe man erkennen müssen, dass dieses Anliegen missverständlich formuliert gewesen sei. Die Sparkasse sagte zu, den Text der Information abzuändern.

22.4 Besonderer Kundenservice

Eine Sparkasse fügte in einigen Fällen den Überweisungsaufträgen ihrer Kunden die komplette Adresse des Auftraggebers automatisch hinzu. Wenn die Angaben auf dem Überweisungsbeleg unleserlich waren, ersetzte die Sparkasse diese Angaben durch den zum Konto hinterlegten Datensatz, wozu auch die vollständige Adresse gehörte. Der Überweisungsempfänger konnte auf seinem

Kontoauszug daher sofort die Adresse des Einzahlers ablesen. Aus Sicht des LfD bestanden gegen ein solches Verfahren datenschutzrechtliche Bedenken. Die Kenntnis der Adresse ist für den Überweisungsempfänger nicht erforderlich. Der Kunde hat die Möglichkeit, beim Verwendungszweck entsprechende Angaben zu machen, die dem Überweisungsempfänger die Zuordnung der Zahlung erlauben. In einigen Fällen kann es gerade wichtig sein, dass der Zahlungsempfänger die Kundenadresse nicht erfährt. Aufgrund der Beschwerde fand die Sparkasse eine programmtechnische Möglichkeit, auf die Weiterleitung der kompletten Adressdaten zu verzichten.

22.5 Gefährliche Praktikantin

Die Kundin einer Sparkasse legte dem LfD einen Ausdruck vor, aus dem sich ihre Kontostände zu einem bestimmten Stichtag bei der Sparkasse ergaben. Mit diesem Ausdruck sei sie anonym bei Gericht angezeigt worden, um ihr Nachteile zuzufügen. Erst auf Nachfrage des LfD rekonstruierte die Sparkasse den Sachverhalt: Eine minderjährige Praktikantin, die denselben Nachnamen wie die Petentin trug, hätte den fraglichen Ausdruck an einem vorübergehend nicht gesperrten PC-Arbeitsplatz eines Mitarbeiters gefertigt. Zwar konnte mit Hilfe der Protokolldaten der unberechtigte Zugriff auf personenbezogene Daten nachvollzogen werden. Hierzu hätte es aber nicht kommen müssen, wenn sich alle Mitarbeiter der Sparkasse an die bestehende Anweisung gehalten hätten, den PC stets bei Verlassen des Arbeitsplatzes zu sperren. Der Vorfall war Anlass genug, den betroffenen Mitarbeiter ausdrücklich auf sein Fehlverhalten hinzuweisen sowie alle Mitarbeiter erneut zu sensibilisieren.

23. Sonstiges

23.1 Sozialkartenverfahren

Mit einem Bündnis will das Land Rheinland-Pfalz gemeinsam mit den rheinland-pfälzischen Tarifvertragsparteien der Bauwirtschaft und mit der Zollverwaltung gegen illegale Beschäftigung und Schwarzarbeit am Bau vorgehen. Teil dieses Bündnisses soll die Erprobung eines Signatur-Kartenverfahrens als Modellprojekt des Bundes in Teilen von Rheinland-Pfalz in einem Praxistest sein.

Hintergrund dieser Bemühungen ist, dass insbesondere in der Baubranche in den vergangenen Jahren zahlreiche Arbeitsplätze durch Schwarzarbeit und illegale Beschäftigung vernichtet wurden. Von 1995 bis 2004 ist nach Angaben der zuständigen Ministerin die Zahl der Arbeitsplätze in der Baubranche von 50 000 auf 38 000 Stellen gesunken; diese Entwicklung sei zu einem erheblichen Maße auf illegale Beschäftigung und Schwarzarbeit zurückzuführen.

Das im Mai 2005 gegründete Bündnis in Rheinland-Pfalz geht zurück auf entsprechende bundesweite Vereinbarungen zur Bekämpfung von illegaler Beschäftigung und Schwarzarbeit. Im Mittelpunkt steht dabei die verstärkte Zusammenarbeit der beteiligten Partner, wie Arbeitgeber, Gewerkschaften und Kontrollbehörden. Auch soll der Einsatz einer so genannten Signatur-Karte (der „Sozialkarte“) geprüft werden.

Ziele des Sozialkartenverfahrens sind:

- Vereinfachung des Zugriffs der Schwarzarbeit bekämpfenden Bediensteten auf die Datenbestände, die bereits jetzt im – sei es automatisierten, sei es herkömmlichen – Zugriff stehen;
- Schaffung eines automatisierten Zugriffsverfahrens auf Datenbestände, die bislang noch nicht im online-Betrieb verfügbar sind;
- Schaffung von automatisiert auswertbaren Datenbeständen in Bereichen, die bislang zwar im herkömmlichen Zugriff stehen, aber nicht automatisiert auswertbar sind, z. B. Gewerberegister, Handwerksrolle;
- automatisierte Abgleiche von Datenbeständen zur Verdachtsgewinnung („Rasterfahndungen“);
- eindeutige Identifikationsmöglichkeiten von Betroffenen durch einen Ausweis mit biometrischen Merkmalen.

Betroffene des Verfahrens (im datenschutzrechtlichen Sinn) sollen zunächst die auf dem Bau tätigen Personen sein, sowohl abhängig Beschäftigte wie selbständige Unternehmer. Eine Ausweitung auf weitere Branchen (wie Lebensmittelbranche etc.) ist denkbar.

Im Pilotverfahren soll allein auf der Basis der – insbesondere auch auf ausreichender Information beruhenden – Einwilligung gearbeitet werden. In Rheinland-Pfalz stehen ca. 30 Unternehmen der Bauwirtschaft mit ca. 500 Beschäftigten dafür zur Verfügung. Getestet werden soll in erster Linie die technische Machbarkeit der ins Auge gefassten Lösungen.

Derzeit handelt es sich bei diesem Projekt um Vorfeldplanungen, deren Realisierbarkeit völlig offen ist. Ursprünglich war insbesondere auch daran gedacht worden, die Daten des Jobcard-Verfahrens (s. Tz. 23.2) in diesem Zusammenhang zu nutzen.

Aus Datenschutzsicht sind jedenfalls bereits jetzt besonders folgende Punkte hervorzuheben:

- Die Datenbestände des Jobcard-Verfahrens können schon aus technischen Gründen für die Schwarzarbeitsbekämpfung nicht genutzt werden, da auf sie nur mit Hilfe des Betroffenen zugegriffen werden kann. Bei Schwarzarbeitskontrollen kommt es aber aus der Sicht der zuständigen „Finanzkontrolle Schwarzarbeit“ (FKS, einer Einrichtung des Zolls) besonders darauf an, schnelle Überprüfungen auch ohne Mitwirkung des Betroffenen durchführen zu können. Es kommt hinzu, dass diese Daten einem völlig anderen Zweck dienen sollen. Sie sollen unter Mitwirkung des Betroffenen dessen Ansprüche auf staatliche Leistungen unterstützen. Eine grundsätzliche Änderung der Zweckbestimmung der hierfür zentral gespeicherten Daten würde eine andere Beurteilung der Verhältnismäßigkeit des in den Datenspeicherungen liegenden Informationseingriffs begründen.

- Grundlage der datenschutzrechtlichen Beurteilung eines solchen Projekts ist in erster Linie die Frage, welche Datenverarbeitungen in welcher Form von wem mit welcher konkreten Zielsetzung und auf welcher Rechtsgrundlage verändert oder neu geschaffen werden sollen. Dies ist die Voraussetzung, um beurteilen zu können, ob dafür die bestehenden Rechtsgrundlagen ausreichen, ob neue Rechtsgrundlagen geschaffen werden müssen und insbesondere auch, ob das Gesamtergebnis verfassungskonform gestaltet werden kann. Die Antworten auf alle diese Fragen sind noch unklar, eine Projektbeschreibung, aus der diese Fakten hervorgehen würden, existiert derzeit noch nicht.
- Konzeptionell ist aus Datenschutzsicht vorzusehen, dass automatisierte Abfrage- bzw. Abgleichsmöglichkeiten am typischen Ablauf einer FKS-Kontrolle zu orientieren sind (gestuftes Verfahren). Dies bedeutet, dass in Fällen, in denen das Ergebnis einer Abfrage einen Schwarzarbeitsverdacht entfallen lässt, nachfolgende Abfragen oder Abgleiche nicht durchlaufen werden.
- Für das Pilotprojekt ist ebenfalls zu konkretisieren, wessen Daten aus welchen Datenbeständen in welcher Form wie verarbeitet und wie (von wem) genutzt werden sollen. Erst auf der Grundlage dieser Festlegungen kann dann eine Einwilligungserklärung formuliert werden, die als ausreichende Rechtsgrundlage für die im Rahmen des Pilotprojekts beabsichtigte Datenverarbeitung dienen kann.

Auch weitere Grundsatzfragen sind nach wie vor unklar, z. B.:

- Welche Bedeutung hat die Schaffung einer neuen Karte mit Signaturfunktion? Ist sie für die Identifizierung wichtig, für den Abruf von Datenbeständen oder aus sonstigen Gründen? Ist sie wirklich zur Zweckerreichung erforderlich oder durch andere Maßnahmen (beispielsweise die Pflicht zur Mitführung allgemeiner Identifikationspapiere auf der Arbeitsstelle – Pass, Personalausweis –) ersetzbar?
- Sollen neue zentrale Datenbestände, wenn ja, mit welchem Inhalt geschaffen werden? Ggf.: in welchem Umfang sind diese wirklich erforderlich?

Zur Beurteilung, ob die Einwilligungserklärung der betroffenen Arbeitnehmer im Rahmen des Testverfahrens (des Pilotprojekts in Rheinland-Pfalz) im Verhältnis zu den teilnehmenden Arbeitgebern eine ausreichende Rechtsgrundlage für Datenverarbeitungen (hier wohl insbesondere Datenübermittlungen) bietet, ist die ADD bzw. das rheinland-pfälzische Innenministerium zuständig.

Über diese vorläufige Einschätzung hat der LfD die Projektbeteiligten unterrichtet.

Es soll ein Projektbeirat unter Teilnahme der Bündnispartner und des Datenschutzes geschaffen werden, der das Verfahren weiter begleitet.

23.2 Das Jobcard-Verfahren

Die Bundesregierung verfolgt das Ziel, ab dem 1. Januar 2007 die Ausstellung von Arbeitsbescheinigungen durch die Arbeitgeber mit Hilfe einer Signaturkarte für alle abhängig Beschäftigten zu zentralisieren und zu vereinfachen.

Das bisher verfolgte Konzept eines JobCard-Verfahrens basiert auf dem Gedanken, Arbeitgeber von der Ausstellung von Bescheinigungen in Sozialleistungsverfahren dadurch zu entlasten, dass sämtliche hierfür relevanten Arbeitnehmerdaten (z. B. zu Gehalt, Arbeitszeiten) in einer Zentralen Speicherstelle (ZSS) gespeichert werden, auf die insbesondere die Sozialleistungsträger im Bedarfsfall nach Autorisierung durch den Betroffenen und durch den jeweiligen Mitarbeiter mit Hilfe von digitalen Signaturkarten Zugriff nehmen können.

Zwar existiert die technische Möglichkeit, die Daten der ZSS auch ohne Mitwirkung der Betroffenen mithilfe eines zentralen Schlüssels zu entschlüsseln. Dies soll aber nur höchst ausnahmsweise und unter Beachtung besonderer Verfahrensvoraussetzungen erfolgen (z. B. im Fall einer technisch bedingten Umschlüsselung aller Datensätze). Die Einbeziehung der Betroffenen ist für den Regelfall im Verfahren zwangsläufig vorgegeben. Nur diese sollen mit ihrer Signaturkarte die Freischaltung ihrer Daten zum Abruf und zur Nutzung erlauben können.

Die Datenschutzbeauftragten des Bundes und der Länder haben folgende Vorgehensweise zur Verbesserung des Datenschutzes vorgeschlagen: Um zu verhindern, dass unbefugt bei der ZSS oder bei angeschlossenen Stellen Beschäftigtendaten verarbeitet werden, sind diese mit einem öffentlichen Schlüssel des Arbeitnehmers durch den Arbeitgeber zu verschlüsseln und so bei der ZSS anzuliefern. Eine Entschlüsselung soll nur über den privaten Schlüssel des Arbeitnehmers möglich sein, der diesen anlässlich der Vorsprache beim Sozialleistungsträger zur Verfügung stellt. Es muss gewährleistet werden, dass der auf der Karte wie der im Trustcenter gespeicherte private Schlüssel von Dritten nicht abgefordert werden darf. Insbesondere müsste eine Beschlagnahmesicherheit des privaten Schlüssels gewährleistet werden. Die Betroffenen sollten faktisch, nicht nur rechtlich die Einzigen sein, die über ihren privaten Schlüssel und damit über ihre Daten verfügen können (Modell der „Ende zu Ende-Verschlüsselung“).

Es zeichnet sich leider ab, dass dieses Modell nicht praxistauglich sein dürfte. In diesem Sinn hat sich das BSI als unabhängiger Gutachter nach intensiver Prüfung geäußert. Aus einer Vielzahl von Gründen (Probleme bei einem Kartenwechsel des Arbeitnehmers, bei einer technisch erforderlichen Neuverschlüsselung, bei einem Kartenverlust des Arbeitnehmers etc.) erscheint diese datenschutzrechtlich vorzugswürdige Gestaltung als nur schwer oder überhaupt nicht realisierbar.

Allerdings ist es aus der Sicht des LfD nach seinem bisherigen Informationsstand erreichbar, sonstige technische und rechtliche Schranken des Verfahrens zu schaffen, durch die ein Schutzniveau erzielt werden kann, das dieses Verfahren als dennoch akzeptabel erscheinen lässt.

So ist die Nutzung der Daten der Beschäftigten ausschließlich auf die Verfahren zu beschränken, an denen der Betroffene mitwirkt. Eine Nutzung dieses bundesweiten Beschäftigtenverzeichnisses durch andere, z. B. private Einrichtungen, und zu anderen Zwecken ist auszuschließen.

Um sicherzustellen, dass der Betroffene Kenntnis über die Entscheidungsgrundlagen im Sozialleistungsverfahren erlangt, ist dieser über den Inhalt der jeweils durch ihn freigegebenen Daten – zumindest auf Anforderung – durch Aushändigung eines Ausdrucks der abgerufenen Daten zu unterrichten.

Der Grundansatz dieses Verfahrens, dass der technische Zugang zu den Daten grundsätzlich nur über den privaten Schlüssel des Betroffenen erfolgt und er insofern die Bestimmungsmöglichkeit über seine Daten in seinen Händen behält, ist datenschutzrechtlich als positiv anzusehen.

Ein solches Verfahren, das sowohl für sämtliche Arbeitgeber (als Datenlieferanten) wie auch für alle abhängig Beschäftigten (als Betroffene) verpflichtend sein soll, muss mit den Grundsätzen, die das Bundesverfassungsgericht zum Recht auf informationelle Selbstbestimmung entwickelt hat, vereinbar sein. In diesem Sinn hat der LfD an der begleitenden Arbeitsgruppe der Datenschutzbeauftragten mitgewirkt; dafür wird er sich auch weiterhin einsetzen.

24. Schlussbemerkung

24.1 Zur Situation der Geschäftsstelle

Wie alle Behörden des Landes hat auch der LfD Einsparungen seines Haushalts erbringen müssen. Trotzdem konnte er seinen gesetzlich festgelegten Auftrag erfüllen. Dies war möglich dank der von der Landtagsverwaltung (z. B. Personalabteilung, Druckerei, Poststelle) erbrachten technischen und administrativen Unterstützung und der Übertragung eines Teils der jeweils im Vorjahr bewilligten nicht verbrauchten Haushaltsmittel in das jeweils neue Haushaltsjahr. So war es möglich, die technische Ausrüstung der Geschäftsstelle zu verbessern und Fortbildungsmöglichkeiten wahrzunehmen. Für alle geleisteten Hilfen ist dem Präsidenten und dem Direktor des Landtags sowie der Landtagsverwaltung aufrichtig zu danken. Das reibungslose Funktionieren der wiederum größer gewordenen Beratungs- und Kontrolltätigkeiten verdankt der LfD vor allem dem engagierten Einsatz der hochmotivierten Mitarbeiterinnen und Mitarbeiter der Dienststelle, die ihre Arbeit sachkundig, umsichtig und zügig erledigt haben. Ihnen gebührt dafür Anerkennung und Dank.

24.2 Zur Öffentlichkeitsarbeit des LfD

Zum Hauptmittel der Öffentlichkeitsarbeit des LfD ist sicherlich sein Internet-Angebot geworden, zu dem unter Tz. 24.3 Näheres ausgeführt wird. Er hat daneben auch traditionelle Öffentlichkeitsarbeit betrieben: so hat er wieder zu den jeweils aktuellsten und aus seiner Sicht wichtigsten Themen Presseerklärungen veröffentlicht.

Zu einer Reihe von Themen hat er Interviews mit Journalisten für Zeitungen und für Hörfunk und Fernsehen gegeben sowie auf den Datenschutz betreffenden Veranstaltungen Vorträge gehalten. Im Vordergrund des Interesses standen dabei die Befugnisse der Strafverfolgungsbehörden im Zusammenhang mit DNA-Analysen, mit Abhörmaßnahmen und mit Videoaufzeichnungen. Auch die Frage der Befugnisse der Finanzbehörden gegenüber den Banken und sonstigen Kreditinstituten hat große öffentliche Aufmerksamkeit gefunden.

Der Versand von Informationsmaterial zu datenschutzrechtlichen Grundfragen (insbesondere auch des Textes des Landesdatenschutzgesetzes) spielt trotz des elektronischen Informationsangebots immer noch eine nennenswerte Rolle.

Seine Mitarbeiter haben verschiedene Fortbildungsveranstaltungen durchgeführt.

24.3 Internetangebot des LfD

Das unter www.datenschutz.rlp.de zur Verfügung stehende Internet-Angebot des LfD wurde im Berichtszeitraum ständig aktualisiert und fortgeschrieben. Insbesondere werden die Rechtsgrundlagen sowohl des Bundes als auch des Landes nicht mehr selbst eingepflegt. Vielmehr begrenzt sich die eigene Pflege nunmehr auf Verordnungen und Rundschreiben. Alle übrigen Rechtsgrundlagen wurden mit einem Link auf das Internetangebot der Bundesregierung „www.gesetze-im-internet.de“ bzw. auf das Landesrecht unter „http://rlp.juris.de“ versehen. Diese Vorgehensweise hat den Vorteil, dass Änderungen der Rechtsgrundlagen zeitnaher und mit weniger personellem Aufwand aktuell zur Verfügung stehen. Darüber hinaus wurden im Berichtszeitraum Teile des Internet-Angebots übersetzt und stehen nunmehr auch in englischer Sprache zur Verfügung.

Das Internet-Angebot des LfD dient der rheinland-pfälzischen Verwaltung vorwiegend als Informationsplattform zur Klärung datenschutzrechtlicher Fragen. Darüber hinaus steht seit Dezember 2000 als zentrale Informations- und Anlaufstelle für Datenschutzfragen im Internet unter www.datenschutz.de das sog. Virtuelle Datenschutzbüro zur Verfügung. Dort befindet sich auch ein Diskussionsforum zu aktuellen Datenschutzthemen. Finanziert wird dieses Projekt durch zahlreiche offizielle Datenschutzinstitutionen im In- und Ausland. Neben dem Bundesbeauftragten und fast allen Landesbeauftragten für den Datenschutz sind u. a. die kirchlichen Datenschutzbeauftragten sowie die Datenschutzbeauftragten des SWR und NDR daran beteiligt. Auch der LfD trägt als Projektpartner seinen Teil zur Finanzierung des Virtuellen Datenschutzbüros bei.

24.4 Zusammenarbeit mit anderen Datenschutzinstitutionen

Die bewährte Abstimmung mit den Datenschutzbeauftragten der anderen Länder und dem des Bundes erfolgte wiederum in Arbeitskreisen und den beiden jährlichen Gesamtkonferenzen. Die Ergebnisse dieser Abstimmungsarbeit kommen in den Entschließungen, die als Anlage abgedruckt sind, zum Ausdruck. Hier wird deutlich, dass trotz gelegentlicher Unterschiede in der Betonung von datenschutzrechtlichen Aspekten ein großer Vorrat an Gemeinsamkeiten besteht.

Die im Berichtszeitraum wiederholte Zusammenarbeit und Abstimmung mit dem Ältestenrat des Landtags bzw. dem Datenschutzbeauftragten der Landtagsverwaltung gestaltete sich effizient und vertrauensvoll.

Im Berichtszeitraum fand erneut ein Treffen mit den Mitarbeitern der ADD statt, die die Funktionen der Aufsichtsbehörde nach § 38 BDSG für nicht-öffentliche Stellen des Landes wahrnimmt. Diese Tätigkeit und die Kontrolltätigkeit des LfD nach den Bestimmungen des Landesdatenschutzgesetzes wirft in einigen Bereichen die gleichen datenschutzrechtlichen Fragen auf, wenn auch die zu überprüfenden Institutionen unterschiedlich sind. Daher wird ein Erfahrungsaustausch von beiden Institutionen gepflegt.

Erörtert wurden folgende Themen:

- Datenschutz in der gesetzlichen und der privaten Krankenversicherung:
  Einwilligungserklärungen, Vermittlung privater Zusatzversicherungen durch gesetzliche Krankenkassen (§ 194 Abs. 1 a SGB V);
- Gesundheitskarte – Modellprojekt Trier;
- Datenschutz bei Ärzten/Beachtung der ärztlichen Schweigepflicht:
- Fragen der Kontrolldichte, Mindeststandards des Datenschutzes, technisch-organisatorische Aspekte, Bereitstellung eines umfassenden Beratungsangebotes;
- Patientenverwaltungs- und -abrechnungsverfahren im Krankenhausbereich;
- Bericht über aktuelle Kontrolltätigkeit des LfD, Erfahrungsaustausch;
- Abstimmung über die datenschutzrechtlichen Zuständigkeiten bei Videoüberwachungen anlässlich der Fußball-WM 2006;
- Datenschutzrechtliche Zuständigkeit für den Flughafen Frankfurt-Hahn;
- Rechtsstellung, Aufgaben und Befugnisse des LfD im Vergleich zur aufsichtsrechtlichen Tätigkeit der ADD und der Fachaufsichtsbehörden.

Der bewährte Meinungsaustausch mit dem Datenschutzbeauftragten des ZDF (Herrn Christoph Bach) und des SWR (Herrn Prof. Dr. Armin Herb) fand anlässlich der Herausgabe des Berichts des ZDF-Datenschutzbeauftragten statt. Hier wurde erneut eine erfreuliche inhaltliche Übereinstimmung in der datenschutzrechtlichen Bewertung von Fragen festgestellt, die von gemeinsamem Interesse sind.

Auch mit der Arbeit der kirchlichen Datenschutzbeauftragten gibt es einige Gemeinsamkeiten. Für das Gebiet des Landes Rheinland-Pfalz sind dies die Datenschutzbeauftragten für die Evangelische Kirche der Pfalz, für die Evangelische Kirche in Hessen und Nassau, für die Evangelische Kirche im Rheinland, für das Bistum Mainz, für das Erzbistum Köln und das Bistum Limburg und für die Bistümer Trier und Speyer. Deshalb fand im Berichtszeitraum auch hier ein Meinungsaustausch insbesondere zum Datenschutz im Sicherheitsbereich, im Bereich Gesundheit und Soziales, im Schulbereich und bei Internet-Auftritten statt.

Die traditionell besonders engen Kontakte zum hessischen Datenschutzbeauftragten wurden gepflegt und vertieft.

Die Kommission beim Landesbeauftragten für den Datenschutz hat im Berichtszeitraum durch regelmäßige Sitzungen wiederum ihre gesetzliche Aufgabe, den LfD bei der Wahrnehmung seiner Aufgaben zu unterstützen, in engagierter Weise wahrgenommen. Die hierdurch mögliche Rückkoppelung an die Tätigkeit des Landtags ist für die datenschutzrechtlichen Anliegen von großer Bedeutung. Nach 20 Jahren in Diensten des Datenschutzes legte der langjährige Vorsitzende der Kommission, Herr Abgeordneter Franz Josef Bischel, sein Amt als Vorsitzender, das er mit großer sachlicher Kompetenz geführt hat, zum 31. Dezember 2003 nieder. Sein bisheriger Vertreter, Herr Abgeordneter Carsten Pörksen, wurde zum neuen Vorsitzenden gewählt, der das Amt mit seiner langjährigen fachlichen Erfahrung umsichtig und souverän führt. Neben ihm gehören gegenwärtig folgende Mitglieder der Kommission beim Landesbeauftragten für den Datenschutz an: Frau Abgeordnete Marlies Kohnle-Gros, Frau Abgeordnete Heike Raab, Frau Abgeordnete Beate Reich, Herr Abgeordneter Christian Baldauf, Herr Abgeordneter Dr. Peter Schmitz, Herr Abgeordneter Nils Wiechmann und Herr Staatssekretär Hendrik Hering. Der LfD möchte diese Gelegenheit benutzen, sich bei allen für ihre Arbeit in der Kommission nachdrücklich zu bedanken.

24.5 Resümee und Ausblick

Als Fazit der vergangenen beiden Jahre bleibt festzuhalten:

Die rasante technische Entwicklung im IT-Bereich hat sowohl die Chancen für Verwaltung und Wirtschaft zu schnelleren und personalreduzierten Verfahren als auch die damit verbundenen Gefährdungen für Datenschutz und Datensicherheit weiterhin erhöht. Die Tendenz, E-Government in vielen Verwaltungsbereichen möglichst zügig einzusetzen, hat zur Folge, dass nicht überall auch die gesetzlich vorgeschriebenen Sicherheitsstandards beachtet wurden, sei es, dass die technischen Voraussetzungen noch nicht hinreichend entwickelt, sei es, dass deren Kosten (noch) zu hoch waren. Der LfD wurde zwar von den einschlägigen Ministerien und Dienststellen des Landes und seiner Körperschaften erfreulicherweise regelmäßig in die Vorbereitungen der Einführung von neuen IT-Verfahren der Datensammlung, -speicherung, -nutzung und -übermittlung eingeschaltet und konnte auch meist die notwendigen Anforderungen des Datenschutzes durchsetzen, doch sind ihm vor allem dort Grenzen gesetzt, wo derartige neue Verfahren länderübergreifend außerhalb des Landes entwickelt wurden. Es besteht zwar die Möglichkeit, in den einschlägigen Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder die Vorstellung des LfD einzubringen, doch fällt unmittelbare Kontrolle nicht in seine Zuständigkeit. Bei der Übernahme solcher Verfahren durch das Land Rheinland-Pfalz hat sich mehrfach die Notwendigkeit zu datenschutzrechtlichen Nachbesserungen ergeben. Die Behörden haben in diesen Fällen in der Regel den Rat des LfD gesucht, doch waren die technischen Schwierigkeiten, datenschutzgerechte Lösungen zu finden, nicht selten recht hoch und mit zusätzlichen Kosten verbunden, die bei rechtzeitiger Beachtung der Vorschriften des Datenschutzes und übrigens auch der Datensicherheit häufig hätten vermieden werden können. Die bewährte Methode, die Beratung des LfD möglichst frühzeitig in Anspruch zu nehmen, die Behörde des LfD also als Helfer bei der Modernisierung der Verwaltung zu akzeptieren, ist nicht überall so stark ausgeprägt wie in Rheinland-Pfalz.

Bei datenschutzrelevanten Gesetzesvorhaben wurde der LfD regelmäßig rechtzeitig eingeschaltet. So konnten etwa die Anforderungen des Datenschutzes an das POG weitgehend einvernehmlich mit dem ISM abgestimmt werden. Auch in der Verwaltungspraxis hat die Beratungstätigkeit des LfD zugenommen. Als Beispiele seien die Einbindung des LfD anlässlich der Sicherheitsmaßnahmen vor und während des Besuches des amerikanischen Präsidenten Bush in Mainz, die Vorbereitung der Fußball-Weltmeisterschaftsspiele in Kaiserslautern oder das Modellprojekt „elektronische Gesundheitskarte Rheinland-Pfalz“ in der Region Trier genannt.

Insgesamt ist festzustellen, dass die Behörden des Landes und seiner juristischen Personen dem Datenschutz gegenüber aufgeschlossen und von seiner Notwendigkeit im Interesse des Schutzes der Privatsphäre der Bürger durchweg überzeugt sind. Wenn dennoch Verstöße gegen das Datenschutzrecht festgestellt wurden, hat der LfD über die von ihm ausgesprochenen Beanstandungen in der Datenschutzkommission berichtet. Soweit möglich, wurden festgestellte datenschutzwidrige Tatbestände sofort oder in angemessener Zeit beseitigt. Im Übrigen ist zu beobachten, dass die jeweils betroffene Verwaltung bereits bei einer angedrohten Beanstandung regelmäßig bereit ist, die datenschutzrechtlichen Vorgaben zu befolgen.

Gleichwohl hat sich an der Tendenz nichts verändert, im Interesse der Sicherheit vor Angriffen gegen die Bürger durch organisierte Kriminalität und internationalen Terrorismus und von Missbrauch von Sozialleistungen angesichts der Finanzsituation der öffentlichen Hände individuelle Freiheit stärker zu beschränken als früher. Auch der Datenschutz blieb davon nicht unberührt. Das Bundesverfassungsgericht hat in seinen Entscheidungen vor allem zur akustischen Wohnraumüberwachung (BVerfGE 109, 279), zum Zollfahndungsneuregelungsgesetz (BVerfGE 110, 33) und zum Niedersächsischen Sicherheits- und Ordnungsgesetz (Urteil vom 27. Juli 2005, Az. 1 BvR 668/04, NJW 2005, 2603) die Grenzen juristischer Eingriffe in die Persönlichkeitssphäre erneut aufgezeigt und die Unverletzlichkeit dessen Kernbereichs bestätigt. Es hat allerdings diesen Kernbereich hinsichtlich des Schutzes der Wohnung nicht ein für alle Mal räumlich genau festgelegt, sondern nur eine Vermutung für Räume aufgestellt, denen typischerweise oder im Einzelfall die Funktion als Rückzugsbereich der privaten Lebensgestaltung zukommt. Eingriffe sind dann zugelassen, wenn es um Gespräche geht, die ihrem Inhalt nach einen unmittelbaren Bezug zu Straftaten aufweisen (BVerfGE 109, 279, 319 ff.).

Aufgabe des LfD ist es, sich darum zu bemühen, das Grundrecht auf Datenschutz zur Geltung zu bringen. Er muss deshalb darauf achten, dass die vom Bundesverfassungsgericht gesetzten Grenzen für dieses Grundrecht nicht überschritten werden, wozu auch gehört, auf mögliche Gefährdungen einer solchen Grenzüberschreitung durch mangelnde organisatorische oder technische Vorkehrungen aufmerksam zu machen. Dies gilt nicht nur für akute Gefährdungen im Landesbereich, sondern auch für Gefahren für das Grundrecht, die außerhalb des Landes im Bunde oder in der Europäischen Union ihren Ursprung haben. Der LfD hat deshalb auch mit den Datenschutzbeauftragten des Bundes und der Länder zu beabsichtigten Einschränkungen des Persönlichkeitsrechts – etwa zur Überwachung der Telekommunikation im Interesse der öffentlichen Sicherheit – durch Organe der Europäischen Union oder des Bundes Stellung genommen, wenn Auswirkungen auf das Land zu erwarten gewesen wären.

Der LfD betrachtet die weitere Entwicklung des Datenschutzes mit skeptischem Optimismus. Das Datenschutzbewusstsein ist auch dank der Medien sicher stärker als in früheren Jahren verankert. Andererseits ist auch das Sicherheitsbedürfnis der Bürger gestiegen. Auch gehen sehr viele Menschen mit ihrem Persönlichkeitsrecht im Alltag recht sorglos um. Das ändert nichts daran, dass das Recht auf Datenschutz als von der Menschenwürde abgeleitetes Grundrecht hoch bewertet werden muss. Zu den Aufgaben des Gesetzgebers, der vollziehenden Gewalt und der Rechtsprechung gehört es, Grundrechte einerseits und Sicherheit und Haushalt andererseits ausgewogen in Konkordanz zu halten. Der LfD ist überzeugt, dass dies sachgerecht bewältigt werden kann. Daran im Interesse des Grundrechts auf Datenschutz mitzuwirken, bleibt seine Verpflichtung.

Anlage 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 21. November 2003
Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz (TKG) beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Anlage 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 13. Februar 2004

Übermittlung von Flugpassagierdaten an die US-Behörden

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z. B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3 ½ Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere acht Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II-System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29. Januar 2004 deutlich herausgearbeitet (http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm):

Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

Anlage 3

Entschließung
der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Anlage 4

Entschließung
der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

Anlage 5

Entschließung
der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Radio-Frequency Identification

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung
der Internationalen Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre vom 20. November 2003 *(Übersetzung)*

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Anlage 6

Entschließung
der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

Anlage 7

Entschließung
der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnen und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Anlage 8

Entschließung
der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Anlage 9

Entschließung
der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Anlage 10

Entschließung
der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20. September 2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Anlage 11

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004

Staatliche Kontenkontrolle muss auf den Prüfstand

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BAföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; aufgrund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben, direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Anlage 12

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005
zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse.

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nichtcodierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nichtcodierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

Anlage 13

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. März 2005

Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Anlage 14

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. März 2005

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Anlage 15

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005

Einführung biometrischer Ausweisdokumente

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. 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,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass 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,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Anlage 16

Presseerklärung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Wirksamer Schutz für genetische Daten

Im Zusammenhang mit den Arbeiten an einem Gendiagnostikgesetz wird über ein Verbot heimlicher Vaterschaftstests diskutiert. Genetische Daten sind besonders schutzwürdig. Die Konferenz unterstützt deshalb den Vorschlag, die heimliche Durchführung von Gentests gesetzlich zu untersagen. Dies gilt sowohl für heimliche Vaterschaftstests als auch für sonstige Gentests, die ohne Wissen der Betroffenen durchgeführt werden.

Durch einen Gentest kann sich heute jede interessierte Person Aufschlüsse über die gesundheitliche Disposition oder biologische Verwandtschaftsverhältnisse verschaffen. Es handelt sich hierbei um Daten aus den intimsten Bereichen eines Menschen, die einen wirksamen Schutz benötigen. Das dafür erforderliche Zellmaterial kann von einem weggeworfenen Zigarettenstummel, einem ausgerissenen Haar oder einem benutzten Trinkglas stammen. Da bis vor kurzer Zeit Gentests noch sehr aufwändig und teuer waren, bestand die Gefahr eines Missbrauchs eher theoretisch. Inzwischen sind Gentests für viele erschwinglich.

Um den Missbrauch zu verhindern, dürfen Gentests nur durchgeführt werden, wenn die Betroffenen wirksam einwilligen oder wenn eine gerichtliche Anordnung auf Basis einer gesetzlichen Ermächtigungsgrundlage vorliegt. Bei allem Verständnis für das Interesse des Vaters an der Feststellung seiner Vaterschaft müssen die elementaren Persönlichkeitsrechte des Kindes geschützt bleiben. Der Ausgleich von unterschiedlichen Interessen kann nicht durch heimliche Gentests sondern nur im Rahmen gesetzlicher Regelungen erfolgen.

Dies alles spricht für ein generelles Verbot heimlicher Gentests, wie es von den Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren gefordert wird. (Siehe Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Gesetzliche Regelungen von genetischen Untersuchungen.)

Anlage 17

Rechtliche Aspekte des Datenschutzes zur Vorratsdatenspeicherung

Vorbemerkung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Deutschland hat sich bereits am 24. Oktober 2002 in ihrer Entschließung „Zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet“ und in ihrer Entschließung „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“ vom 21. November 2003 gegen die Einführung einer Vorratsspeicherung von Verkehrsdaten ausgesprochen. Nicht zuletzt haben die deutschen Datenschutzbeauftragten in einer gemeinsamen Presseerklärung vom 25. Juni 2004 die Initiative Großbritanniens, Irlands, Frankreichs und Schwedens für einen Rahmenbeschluss des Rates der EU im Rahmen der dritten Säule kritisiert. Auch die Konferenz der europäischen Datenschutzbeauftragten lehnt die Einführung einer Vorratsdatenspeicherung ab (Entschließung vom 9. bis 11. September 2002). Vor dem Hintergrund dieser grundsätzlichen Äußerungen hat es der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder übernommen, im Rahmen der öffentlichen Konsultation der Europäischen Kommission Stellung zu nehmen.

Derzeitige Praxis in Deutschland

Speicherung für eigene Zwecke

Nach derzeitiger Rechtslage richtet sich die Speicherung von Verkehrsdaten im Sinne von Art. 6 der Richtlinie 2002/58/EG in Deutschland nach unterschiedlichen Gesetzen. Insofern bestehen keine einheitlichen Bestimmungen für den Datenschutz im Bereich der elektronischen Kommunikation.

Zu unterscheiden ist die Verarbeitung von Verkehrsdaten im Bereich der Telekommunikation von der Verarbeitung von Nutzungsdaten bei der Inanspruchnahme von Tele- und Mediendiensten. Während Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen ist (§ 3 Nr. 22 Telekommunikationsgesetz [TKG]), sind Tele- und Mediendienste Informations- und Kommunikationsdienste, denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Es handelt sich bei letzteren also um „höherwertige“ Dienste, die auf der Telekommunikation im engeren Sinne aufsetzen. Dazu gehört insbesondere die Nutzung des Internet. Gleichwohl handelt es sich bei den Nutzungsdaten im Bereich der Tele- und Mediendienste um Verkehrsdaten im Sinne der Richtlinie 2002/58/EG.

In diesem Sinne werden als Verkehrsdaten nach dem TKG solche Daten angesehen, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, § 3 Nr. 30 TKG. Dies sind z. B. Telefonnummern, Berechtigungskennungen, Kartennummern, IMSI, IMEI, Standortdaten (z. B. Funkzelle), Beginn und Ende der Verbindung nach Datum und Uhrzeit, Datenmengen, Endpunkte von Festverbindungen sowie deren Beginn und Ende nach Datum und Uhrzeit. Je nach Verwendungszusammenhang finden auf IP-Adressen auch die Regelungen des Tele- bzw. Mediendiensterechts Anwendung. IP-Adressen sind in jedem Falle Verkehrsdaten im Sinne der Richtlinie 2002/58/EG.

Rechtsgrundlagen für die Verarbeitung von Verkehrs- und Nutzungsdaten sind §§ 96 ff. Telekommunikationsgesetz (TKG) für Verkehrsdaten sowie § 6 Teledienstedatenschutzgesetz (TDDSG) und § 19 Abs. 2 bis 9 Mediendienste-Staatsvertrag (MDStV) für Nutzungsdaten.

Allen Vorschriften ist gemeinsam, dass Verkehrs- bzw. Nutzungsdaten unverzüglich nach Ende der Verbindung grundsätzlich zu löschen sind. Eine Speicherung über das Ende der Verbindung hinaus ist nur als Ausnahme zulässig. Die Ausnahmeregelungen enthalten jeweils nur die Befugnis, in keinem Falle aber die Verpflichtung, Verkehrs- oder Nutzungsdaten zu speichern. Auf eine Vorratsdatenspeicherung ist bei der kürzlich – u. a. in Umsetzung der Richtlinie 2002/58/EG – erfolgten Novellierung des TKG trotz entsprechender Forderungen des Bundesrates sowie der Sicherheitsbehörden aus verfassungsrechtlichen Gründen bewusst verzichtet worden (dazu s. u.).

Wichtigste Ausnahme zur Speicherung von Verkehrs- und Nutzungsdaten über das Ende der Verbindung hinaus ist die Speicherung zu Zwecken der Abrechnung in Anspruch genommener Dienste, vgl. § 97, 99 TKG bzw. § 6 Abs. 4 bis 7 TDDSG und § 19 Abs. 3 bis 8 MDStV. Auch diesen Vorschriften ist gemeinsam, dass Verkehrs- und Nutzungsdaten nur gespeichert werden dürfen, wenn dies für Zwecke der Abrechnung erforderlich ist, d. h. die Abrechnung ohne die Nutzung dieser Daten nicht möglich wäre. Es hängt damit vom konkreten Abrechnungsverfahren ab, ob und welche Verkehrs- und Nutzungsdaten gespeichert werden dürfen. So ist etwa bei Pauschaltarifen (flatrates) eine Speicherung von Verkehrsdaten regelmäßig nicht erforderlich und damit unzulässig.

Abrechnungsdaten dürfen von den Anbietern maximal sechs Monate nach Versendung der Rechnung gespeichert werden. Eine Pflicht zur Speicherung besteht nicht (s. o.). In der Praxis wird die Frist bei den bedeutenden Telekommunikationsunternehmen in der Regel nicht ausgenutzt, im Durchschnitt wird etwa drei Monate gespeichert. Den Nutzern stehen verschiedene Wahlrechte hinsichtlich der Speicherung von Verkehrs- und Nutzungsdaten zum Zwecke der Abrechnung zur Verfügung.

Außer zu Abrechnungszwecken dürfen Verkehrsdaten in der Telekommunikation ohne Einwilligung des Nutzers im Einzelfall nur zur Abwehr von Störungen und Missbräuchen und zur sog. Fangschaltung bei Bedrohungen oder Belästigungen gespeichert und verarbeitet werden (§§ 100, 101 TKG). Nutzungsdaten von Tele- und Mediendiensten dürfen außer zur Abrechnung nur bei Verdacht der betrügerischen Inanspruchnahme des Dienstes verarbeitet werden (§ 6 Abs. 8 TDDSG, § 19 Abs. 9 MDStV).

Zugriff von Sicherheitsbehörden

Im Strafverfahren stehen den Staatsanwaltschaften als Ermittlungsbehörden die Befugnisse nach § 100 g, 100 h Strafprozessordnung (StPO) zur Verfügung. Nach § 100 g StPO kann angeordnet werden, dass Anbieter Verkehrsdaten herausgeben müssen, wenn jemand im Verdacht steht, eine Straftat von erheblicher Bedeutung oder eine Straftat mittels einer Endeinrichtung begangen zu haben. Der Staatsanwalt muss dafür eine richterliche Anordnung beantragen, in der Name, Anschrift, Rufnummer oder eine andere Kennung des Betroffenen zu nennen sind. Im Falle von Straftaten erheblicher Bedeutung genügt die Angabe einer räumlich und zeitlich hinreichend bestimmten Kommunikation.

Die Staatsanwaltschaft erhält aus vergangenen Kommunikationen selbstverständlich nur Daten, die beim Anbieter noch vorhanden sind. Eine Anordnung in die Zukunft – mit entsprechender Speicherpflicht – ist zulässig.

Die Geheimdienste können nach dem G-10-Gesetz unter bestimmten Voraussetzungen die Herausgabe von Verkehrsdaten beim zuständigen Bundes- oder Landesminister beantragen. Dieser ordnet die Herausgabe durch die Anbieter an. Die Anordnungen werden von parlamentarischen Ausschüssen kontrolliert.

Auch hier können nur Daten herausgegeben werden, die aufgrund der o. g. Befugnisse der Anbieter noch vorhanden sind.

Eine Pflicht zur Vorratsspeicherung von Verkehrsdaten im staatlichen Interesse existiert in Deutschland nicht.

Einführung einer Vorratsspeicherung von Verkehrsdaten in Deutschland und der EU

Das Ziel der Kommission, einen europaweit einheitlichen Umgang mit Verkehrsdaten in einem gemeinsamen Binnenmarkt zu erreichen, ist auch aus Sicht der Datenschutzbeauftragten in Deutschland zu begrüßen.

Dies kann sich jedoch nur auf die Verarbeitung zu betrieblichen Zwecken beziehen. Hier ist mit der Richtlinie 2002/58/EG eine ausreichende Harmonisierung vorgenommen worden. Art. 15 dieser Richtlinie enthält keine Befugnis zur Vorratsspeicherung von Verkehrsdaten und auch keine Verpflichtung der Mitgliedsstaaten, eine solche Befugnis einzuführen.

Nur im Rahmen der dritten Säule der EU ist es denkbar, eine Harmonisierung der staatlichen Zugriffsbefugnisse auf Verkehrsdaten zu erreichen.

Es bestehen erhebliche Zweifel, ob eine Vorratsdatenspeicherung, wie sie auch im o. g. Entwurf des Rates für einen Rahmenbeschluss vorgesehen ist, mit Art. 8 der Europäischen Menschenrechtskonvention (EMRK) vereinbar ist.

Art. 8 EMRK garantiert das Menschenrecht auf Schutz des Privatlebens und der Korrespondenz; er lässt Eingriffe in die Ausübung dieses Recht nur zu, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Die Pläne zur Vorratsdatenspeicherung stützen sich ausschließlich auf den Zweck der Verhütung (einschließlich der Untersuchung, Feststellung und Verfolgung) von Straftaten.

Der Europäische Gerichtshof für Menschenrechte (und ihm folgend auch der Gerichtshof der Europäischen Gemeinschaften) hat die Schrankenklausel des Art. 8 Abs. 2 EMRK stets sehr eng ausgelegt und nur solche Eingriffe als in einer demokratischen Gesellschaft „notwendig“ angesehen, für die ein zwingender gesellschaftlicher Bedarf („pressing social need“) besteht (vgl z. B. die Entscheidung Klass ./. Bundesrepublik Deutschland v. 18. November 1977, European Court of Human Rights, Series A no. 28). Der Gerichtshof für Menschenrechte hat die Befugnis der Vertragsstaaten anerkannt, in Ausnahmefällen und unter besonderen Umständen die Korrespondenz und Telekommunikation von Personen auch heimlich zu überwachen. Er hat aber wörtlich hinzugefügt:

„… dies bedeutet nicht, dass die Vertragsstaaten ein unbeschränktes Ermessen haben, Personen in ihrem Hoheitsgebiet einer heimlichen Überwachung zu unterwerfen. Angesichts der Tatsache, dass entsprechende Befugnisse mit der Begründung, die Demokratie verteidigen zu wollen, diese gerade zu unterminieren oder zu zerstören drohen, betont der Gerichtshof, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten.“

Die im o. g. Entwurf für einen Rahmenbeschluss des Rates vorgesehene Verpflichtung zur routinemäßigen, flächendeckenden Vorratsdatenspeicherung sämtlicher Verkehrs-, Nutzer- und Teilnehmerdaten würde die ausnahmsweise zulässige Überwachung zur evident unverhältnismäßigen Regel machen. Der Entwurf weist z. B. selbst darauf hin, es sei „erforderlich, bestimmte Datentypen, die zu rechtmäßigen Zwecken verarbeitet werden, während eines bestimmten zusätzlichen Zeitraums aus der Überlegung heraus auf Vorrat zu speichern, dass sie für künftige Ermittlungen oder Gerichtsverfahren erforderlich sein könnten“ (Erwägungsgrund 6). Solche Überlegungen rechtfertigen die vorgesehenen Eingriffe im Sinne des Art. 8 Abs. 2 EMRK nicht, denn dazu müssten sie im Einzelfall erforderlich sein, ein entsprechendes Erfordernis dürfte keine bloße zukünftige Möglichkeit sein. Eine Erleichterung der

Zusammenarbeit der Mitgliedstaaten und ein harmonisiertes Reglement ist sicherlich wünschenswert. Das führt in einer demokratischen Gesellschaft aber nicht dazu, dass eine systematische Registrierung des gesamten elektronischen Kommunikationsverhaltens zulässig sein kann.

In Deutschland verstieße die Einführung einer gesetzlichen Verpflichtung, Verkehrsdaten für zukünftige und noch unbestimmte Zugriffe der Sicherheitsbehörden auf Vorrat zu speichern, gegen Verfassungsrecht. Das Bundesverfassungsgericht hat im Volkszählungsurteil eine Speicherung zu noch unbestimmten Zwecken generell für verfassungswidrig erklärt (BVerfGE 65, 1, 46). Bei einer Vorratsdatenspeicherung impliziert bereits der Begriff, dass die konkreten Zwecke der Speicherung nicht vorhergesehen werden können. Im Gegenteil, in der überwiegenden Zahl aller Fälle werden und sollen die Verkehrsdaten der Teilnehmer gar nicht genutzt, aber gleichwohl nach den Vorstellungen der Initiative über einen längeren Zeitraum ohne jede Zweckbestimmung gespeichert und zum Zugriff bereit gehalten werden.

Die Verpflichtung zur Vorratsspeicherung sämtlicher Verkehrsdaten ist insbesondere mit Art. 10 GG unvereinbar, weil sie alle Teilnehmer der elektronischen Kommunikation in Anspruch nimmt und damit unter Generalverdacht einer Straftat stellt. Das Bundesverfassungsgericht hat zuletzt in seinem Urteil vom 12. März 2003 (1 BvR 330/96, 348/99 – ZDF/Stern – BVerfGE 107, 299) zur Speicherung und Verwendung von Verbindungsdaten für die Bekämpfung schwerer Straftaten betont, dass deren Aufklärung und Verfolgung zwar ein legitimer öffentlicher Zweck und ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens seien, für den Auskünfte nach den §§ 100 a und 100 b StPO eingeholt werden dürften. Es hat aber gleichzeitig betont, dass die damit verbundenen schwerwiegenden Eingriffe in das Fernmeldegeheimnis nur verhältnismäßig im engeren Sinne sind, wenn die Gegenbelange gewichtig und konkret sind. Das Gewicht des Strafverfolgungsinteresses sei insbesondere von der Schwere und der Bedeutung der aufzuklärenden Straftat abhängig. Wörtlich fährt das Gericht dann fort:

„Insofern genügt es verfassungsrechtlichen Anforderungen nicht, dass die Erfassung der Verbindungsdaten allgemein der Strafverfolgung dient. Vorausgesetzt sind vielmehr eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis für die Annahme, dass der durch die Anordnung Betroffene als Nachrichtenmittler tätig wird (BVerfGE 107, 299, 321).“

Diesen Anforderungen genügt eine Vorratsdatenspeicherung etwa nach dem Vorbild des Entwurfs des Rahmenbeschlusses nicht nur nicht, er sucht sie explizit außer Kraft zu setzen. Es soll gerade kein konkreter Tatverdacht und keine hinreichend sichere Tatsachenbasis im Einzelfall gefordert werden, sondern die Vorratsspeicherung pauschal und präventiv für eine mögliche zukünftige Strafverfolgung zulasten aller, die elektronische Kommunikationsnetze nutzen, angeordnet werden. Dies ist mit dem Fernmeldegeheimnis nach deutschem Verfassungsrecht unvereinbar.

Eine über Zwecke des Betriebs hinausgehende Speicherung von Verkehrsdaten ist unverhältnismäßig, denn sie verletzt insbesondere auch den Grundsatz der Erforderlichkeit. Dem Gesetzgeber steht mit dem Instrument des „quick freeze – fast thaw“ ein milderes und grundrechtsschonenderes Mittel zur Verfügung, das eine Speicherung von Verkehrsdaten auf konkrete Anlässe beschränkt. Dieses Instrument ist bereits in der Konvention des Europarates zur Bekämpfung der Datennetzkriminalität (Cybercrime-Konvention) enthalten, aber in zahlreichen Unterzeichnerstaaten – auch in Deutschland – noch nicht umgesetzt worden. Vor weiteren Initiativen mit flächendeckenden Belastungen sollten die Europäische Kommission und der Rat die Umsetzung dieses Instrumentes und seine praktischen Auswirkungen abwarten.

Nach allem können Pläne zur Einführung einer pauschalen Vorratsspeicherung von Verkehrsdaten nur abgelehnt werden.

Anlage 18

Die Datennutzung bei den Forschungsdatenzentren

Um der Wissenschaft den Zugang zum Informationspotential der amtlichen Statistik zu öffnen, richten die Forschungsdatenzentren unterschiedliche Zugangswege ein. Sie resultieren aus verschiedenen Kombinationen von Datenanonymisierung und Zugriffsregulierung:

– Absolut anonymisierte Mikrodatensätze

Absolut anonymisierte Daten werden durch Aggregation oder durch die Entfernung einzelner Merkmale soweit verändert, dass eine Identifizierung der Auskunftgebenden nach menschlichem Ermessen unmöglich gemacht wird. Die amtliche Statistik bietet absolut anonymisierte Mikrodaten in Form sog. Public Use Files an. Diese können allen interessierten Personen zur Verfügung gestellt werden.

– Faktisch anonymisierte Mikrodatensätze

Eine absolute Datenanonymisierung birgt den Nachteil, dass damit auch ein erheblicher Teil der statistischen Information verloren geht. Dagegen werden Mikrodaten als faktisch anonym bezeichnet, wenn die Deanonymisierung zwar nicht gänzlich ausgeschlossen werden kann, die Angaben jedoch nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft dem jeweiligen Merkmalsträger zugeordnet werden können. Diese Regelung geht zurück auf § 16 Abs. 6 BStatG. Wann ein Mikrodatensatz als faktisch anonym bezeichnet werden kann, hängt insbesondere davon ab, unter welchen Rahmenbedingungen die Daten verarbeitet werden. So ist von entscheidender Bedeutung, welches Zusatzwissen vorliegt und wo die Datennutzung stattfindet. Abhängig davon, ob die Mikrodaten extern oder in den statistischen Ämtern genutzt werden, kann die faktische Anonymität mit mehr oder minder starken Informationseinbußen erreicht werden. Da bei der Herausgabe dieser Daten ein höheres Deanonymisierungsrisiko besteht als bei der Nutzung in einem statistischen Amt, ist die Datenanonymisierung relativ stark ausgeprägt. Die für diese Nutzungsform erzeugten Datensätze werden als Scientific Use Files bezeichnet.

– Projektbezogene faktische Anonymisierung zur On-Site-Nutzung

Eine projektbezogene Anonymisierung der Daten hat den praktischen Vorteil, dass dabei nicht die gesamten Ergebnisse einer Statistik anonymisiert werden, sondern lediglich die daraus benötigten Merkmale. Hier wird ebenfalls eine faktische Datenanonymität erzeugt. Diese Daten können jedoch nur in den Räumlichkeiten der Forschungsdatenzentren an sog. Gastwissenschaftlerarbeitsplätzen mit den gängigen statistischen Analyseprogrammen ausgewertet werden.

– Nutzung amtlicher Mikrodaten durch kontrollierte Datenfernverarbeitung

Im Rahmen dieses Verfahrens erstellen Wissenschaftler zu ihren Forschungsvorhaben ein Auswertungsprogramm. Das entsprechende Forschungsdatenzentrum prüft das Programm, lässt es mit den benötigten Daten ablaufen und führt eine Auswertung durch. Zur praktikablen Anwendung der Datenfernverarbeitung stellen die Forschungsdatenzentren Datenstrukturfiles zur Verfügung, die es den Nutzern ermöglichen, ihre Auswertungsprogramme auf die Struktur der Originaldaten abzustimmen. Diese Datenstrukturfiles geben die Struktur des originären Datensatzes wieder, ohne inhaltliche Informationen zu transportieren. Die Wissenschaftler haben somit keinen direkten Kontakt mit den geheimhaltungsbedürftigen Daten. Eine (faktische) Anonymisierung der Daten muss daher nicht vorgenommen werden. Die Ergebnisse werden vor Auslieferung an die Wissenschaftler auf Wahrung der Geheimhaltung geprüft. Sie erhalten nur Datenmaterial, das den Vorschriften der statistischen Geheimhaltung genügt.

Anlage 19

Meldegesetz (MG)
vom 22. Dezember 1982; zuletzt geändert durch Gesetz vom 25. Juli 2005, GVBl. 2005, S. 309

(…)

§ 34
Melderegisterauskunft

(1) Personen, die nicht Betroffene sind, und anderen als den in § 31 Abs. 1 bezeichneten Stellen darf die Meldebehörde nur Auskunft über
1. Vor- und Familiennamen,
2. Doktorgrad sowie
3. Anschriften

einzelner bestimmter Einwohnerinnen und Einwohner erteilen (einfache Melderegisterauskunft). Dies gilt auch, wenn jemand Auskunft über eine Vielzahl namentlich bezeichneter Einwohnerinnen und Einwohner begehrt.

(2) Einfache Melderegisterauskünfte können auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung erteilt werden, wenn
1. der Antrag in der amtlich vorgeschriebenen Form gestellt worden ist,
2. die antragstellende Person oder Stelle die betroffene Person mit Vor- und Familiennamen sowie mindestens zwei weiteren der aufgrund von § 3 Abs. 1 gespeicherten Daten eindeutig bezeichnet hat und
3. die Identität der betroffenen Person durch einen automatisierten Abgleich der im Antrag angegebenen mit den im Melderegister gespeicherten Daten der betroffenen Person eindeutig festgestellt worden ist.

Die der Meldebehörde überlassenen Datenträger oder übermittelten Daten sind nach Erledigung des Antrags unverzüglich zurückzugeben, zu löschen oder zu vernichten. § 9 Abs. 2 Satz 2 gilt entsprechend.

(3) Einfache Melderegisterauskünfte können unter den Voraussetzungen des Absatzes 2 Satz 1 Nr. 1 bis 3 auch mittels automatisierten Abrufs über das Internet erteilt werden; dabei sind die Anforderungen des Standards OSCI-XMeld in der jeweils gültigen Version für die einfache Melderegisterauskunft einzuhalten. Die Antwort an die antragstellende Person oder Stelle ist zu verschlüsseln. Die Eröffnung des Zugangs zum automatisierten Abruf über das Internet ist öffentlich bekannt zu machen. Ein Abruf ist nicht zulässig, wenn die betroffene Person dieser Form der Auskunftserteilung widersprochen hat. Auf die Eröffnung des Zugangs und das Widerspruchsrecht hat die Meldebehörde bei der Anmeldung sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Absatz 2 Satz 3 gilt entsprechend.

(4) Der automatisierte Abruf über das Internet kann statt über den eigenen Zugang der Meldebehörde auch über ein Portal oder mehrere Portale erfolgen. Ein Portal hat insbesondere die Aufgabe,
1. anfragende Personen und Stellen zu registrieren,
2. Auskunftsersuchen entgegenzunehmen, zu bearbeiten und an Meldebehörden oder andere Portale weiterzuleiten,
3. die Antworten entgegenzunehmen, gegebenenfalls zwischenzuspeichern und weiterzuleiten,
4. die Zahlung der Gebühren an die Meldebehörden sicherzustellen und
5. die Datensicherheit zu gewährleisten.

Ein Portal darf die ihm übermittelten Daten nur so lange speichern, wie es für die Erfüllung seiner Aufgaben erforderlich ist. Absatz 2 Satz 3 gilt entsprechend. Wird ein Portal nicht in öffentlich-rechtlicher Form betrieben, bedarf es der Zulassung durch das für das Melderecht zuständige Ministerium. Soweit Auskünfte nach Absatz 1 aus dem Integrationssystem nach § 37 oder dem Informationssystem nach § 38 erteilt werden, gelten die Sätze 3 bis 5 entsprechend.

(…)

Begründung

Zu § 34

(…)

Zu Absatz 2

(…)

Unberührt bleibt im Übrigen die Beachtung der allgemeinen Erfordernisse zur Gewährleistung des Datenschutzes und der Datensicherheit. Durch Satz 3 wird insoweit klargestellt, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit zu treffen sind. Dies hat zur Folge, dass das in Satz 2 normierte Gebot der Rückgabe, Löschung oder Vernichtung der Datenträger oder der übermittelten Daten vor allem auch die durch § 9 Abs. 2 Nr. 4 des Landesdatenschutzgesetzes begründete Verpflichtung unberührt lässt, Maßnahmen zu treffen, die gewährleisten, dass vor allem auch durch den Landesbeauftragten für den Datenschutz nachträglich überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt worden sind.

Zu Absatz 3

Satz 1 sieht vor, dass unter den in Absatz 2 Satz 1 Nr. 1 bis 3 genannten Voraussetzungen einfache Melderegisterauskünfte auch mittels eines automatisierten Abrufs über das Internet erteilt werden können. In diesem Fall sind allerdings die Anforderungen des Standards OSCI-XMeld in der jeweils gültigen Fassung einzuhalten.

Zur Vermeidung einer unbefugten Kenntnisnahme von dem Inhalt der jeweiligen Melderegisterauskunft ist in Satz 2 geregelt, dass die Antwort an die Person oder Stelle, die die Melderegisterauskunft beantragt hat, zu verschlüsseln ist.
Mit den Sätzen 3 bis 5 soll § 21 Abs. 1 a Satz 2 MRRG in Landesrecht umgesetzt werden.
Nach Satz 3 ist die Eröffnung der Möglichkeit, Auskunftsersuchen in elektronischer Form über das Internet an das Melderegister zu richten, öffentlich bekannt zu machen.
Nach Satz 4 ist die Erteilung einer Auskunft aus dem Melderegister über das Internet allerdings nur zulässig, wenn Betroffene dieser Form der Auskunftserteilung nicht widersprochen haben. Hat eine Einwohnerin oder ein Einwohner der Erteilung einer einfachen Melderegisterauskunft in elektronischer Form widersprochen, ist die Erteilung einer Auskunft in dieser Form nicht zulässig. Unberührt hiervon bleibt, dass die entsprechenden Auskunftsersuchen nach Absatz 1 in herkömmlicher Form von der zuständigen Meldebehörde bearbeitet werden dürfen.
Auf die Eröffnung des Zugangs zur automatisierten Erteilung von Melderegisterauskünften über das Internet und das Widerspruchsrecht hat die Meldebehörde nach Satz 5 bei der Anmeldung sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.
Durch Satz 6 wird sichergestellt, dass bei der Erteilung von einfachen Melderegisterauskünften über das Internet zu gewährleisten ist, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen sind.

Zu Absatz 4

In dem im Auftrag der Innenministerkonferenz erstellten Bericht der Arbeitsgruppe „Meldewesen“ vom 21. März 2003 ist festgehalten, dass die Mehrzahl der an das Melderegister gerichteten Auskunftsersuchen im privaten Bereich von so genannten Powerusern stammt, das heißt von Rechtsanwältinnen und Rechtsanwälten, Notarinnen und Notaren, Inkassobüros, Versandhäusern und großen Vereinen wie dem ADAC. Vor diesem Hintergrund ist in dem von der Innenministerkonferenz gebilligten Bericht vorgeschlagen worden, die Erteilung einer einfachen Melderegisterauskunft über das Internet statt über den eigenen Zugang der Meldebehörde auch über ein so genanntes Portal zuzulassen. Dem vorgenannten Anliegen wird durch Satz 1 Rechnung getragen.
Ein Portal, das für mehrere Meldebehörden oder auch landesweit eingerichtet werden kann, hat nach Satz 2 insbesondere die Aufgabe, die anfragenden Personen und Stellen zu registrieren, Auskunftsersuchen entgegenzunehmen, zu bearbeiten und an Meldebehörden oder andere Portale weiterzuleiten, die Antworten von Meldebehörden oder anderen Portalen entgegenzunehmen, gegebenenfalls zwischenzuspeichern und weiterzuleiten, die Zahlung der Gebühren an die Meldebehörden sicherzustellen und die Datensicherheit zu gewährleisten. Durch die in Satz 3 vorgesehene Regelung soll sichergestellt werden, dass die bei einem Portal gespeicherten personenbezogenen Daten nur für die Dauer der Aufgabenerledigung gespeichert werden.
Durch den in Satz 4 geregelten Verweis auf Absatz 2 Satz 3 wird im Übrigen klargestellt, dass auch bei der Verarbeitung personenbezogener Daten durch ein Portal die in § 9 Abs. 2 Satz 2 MG genannten Datenschutz- und Datensicherungserfordernisse zu beachten sind. Insoweit lässt das Gebot, die dem Portal übermittelten Daten nur so lange zu speichern, wie es für die Erfüllung seiner Aufgaben erforderlich ist, unter anderem die durch § 9 Abs. 2 Nr. 4 des Landesdatenschutzgesetzes begründete Verpflichtung unberührt, Maßnahmen zu treffen, die gewährleisten, dass insbesondere auch durch den Landesbeauftragten für den Datenschutz nachträglich überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt worden sind.
Satz 5 regelt, dass ein Portal, das nicht in öffentlich-rechtlicher Form betrieben wird, der Zulassung durch das für das Melderecht zuständige Ministerium bedarf.
In Rheinland-Pfalz sind im Rahmen der im Jahr 2003 erfolgten Neuordnung des Meldewesens mit dem in § 37 MG geregelten Integrationssystem und dem in § 38 MG geregelten Informationssystem zwei Verfahren geschaffen worden, die eine landesweit zentrale Erledigung einzelner meldebehördlicher Aufgaben und insbesondere auch die Bearbeitung der Auskunftsersuchen von Powerusern nach Vornahme von technischen Anpassungen im Grundsatz ermöglichen. Insoweit bietet sich an, in Zusammenarbeit mit interessierten Stellen die technischen Voraussetzungen zu schaffen, zukünftig zumindest einen Teil der entsprechenden Auskunftsersuchen, die von Privaten an die 212 Meldebehörden in Rheinland-Pfalz gerichtet sind, automationsgestützt zentral zu bearbeiten. Da sowohl im Integrationssystem als auch im Informationssystem der Bestand mit Grunddaten aller Melderegister in Rheinland-Pfalz dauerhaft vorgehalten wird, werden die in den Sätzen 3 bis 5 getroffenen Regelungen hinsichtlich der Aufgaben eines oder mehrerer Portale nach Satz 6 lediglich für entsprechend anwendbar erklärt. Von einer gesetzlichen Festlegung auf eines der zentralen Systeme für die Wahrnehmung der Portalfunktion soll abgesehen werden, da die entsprechende Entscheidung erst nach einer näheren Prüfung der technischen und organisatorischen Voraussetzungen getroffen werden soll. Dabei ist auch zu berücksichtigen, dass das Integrationssystem im Auftrag der Rechtsträger der Meldebehörden und das Informationssystem außerhalb des Meldewesens in der Verantwortung des Landes betrieben wird.

(…)

Anlage 20

Resolutionen der 27. Internationalen Konferenz der Datenschutzbeauftragten am 16. September 2005 in Montreux

A. Erklärung von Montreux

„Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung;
2. erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschliessung über den Datenschutz und die internationalen Organisationen;
3. stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmaßnahmen beherrscht wird;
4. sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt;
5. verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien;
6. sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt;
7. sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten überhaupt werden können, und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt;
8. erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen;
9. erkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens an, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann;
10. sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft ist;
11. sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist;
12. sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen;
13. sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen;
14. erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat;
15. erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten zehn Geboten zum Schutz der Privatheit Rechnung zu tragen;

16. erkennen an, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC);

17. erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:
    - Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
    - Prinzip der Richtigkeit,
    - Prinzip der Zweckgebundenheit,
    - Prinzip der Verhältnismäßigkeit,
    - Prinzip der Transparenz,
    - Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
    - Prinzip der Nicht-Diskriminierung,
    - Prinzip der Sicherheit,
    - Prinzip der Haftung,
    - Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,
    - Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierungen und den internationalen und supranationalen Organisationen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragen

a) die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;

b) sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäß den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;

c) den Europarat gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern;

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16. bis 18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a) die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzuhalten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;

b) die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;

c) die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten. Die Datenschutzbeauftragten kommen ausserdem überein
    - namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschliessungen der Konferenz zu verstärken;
    - die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;

- den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;
- mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;
- eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

B. Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschliesst:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zurzeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können,

wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis,

unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann,

im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar“ machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten,

unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte,

fordert die Konferenz

1. wirksame Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können;
2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden;
3. die technische Beschränkungen der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

C. Resolution zur Verwendung von Personendaten für die politische Kommunikation

Die Konferenz (zieht)

in Erwägung, dass politische Kommunikation ein grundlegendes Instrument für die Beteiligung der Bürgerinnen und Bürger, der politischen Kräfte und der Kandidatinnen und Kandidaten am Leben einer Demokratie ist, und in Anerkennung der Wichtigkeit der Freiheit der politischen Meinungsäusserung als ein Grundrecht;

in Erwägung, dass gelebte Staatsbürgerschaft das Recht der Bürgerinnen und Bürger voraussetzt, im Rahmen von Wahlkampagnen von Politik und Verwaltung Informationen zu erhalten und angemessen informiert zu werden; in Erwägung, dass diese Rechte auch geeignet sind, um bei weiteren Themen, Ereignissen und politischen Positionen in Kenntnis der Sachlage seine Wahl zu anderen Themen des politischen Lebens treffen zu können, sei es bei Referenden, bei der Wahl von Kandidatinnen und Kandidaten oder beim Zugang zu Informationen innerhalb politischer Organisationen oder von gewählten Amtsträgern;

in Erwägung, dass die politischen Kräfte und politische Organisationen im Allgemeinen sowie gewählte Abgeordnete sich verschiedener Formen der Kommunikation und der Geldmittelbeschaffung bedienen und Informationsquellen und neue Technologien nutzen, um direkte und persönliche Kontakte mit verschiedensten Kategorien von betroffenen Personen zu knüpfen;

in Erwägung, dass in einer wachsenden Zahl von Ländern ein Trend hin zu immer stärkerer institutioneller Kommunikation gewählter Kandidatinnen und Kandidaten und Körperschaften zu beobachten ist, ebenfalls auf lokaler Ebene und mittels E-Government; in der Erwägung, dass diese Aktivitäten, die die Verarbeitung von Personendaten voraussetzen können, in Einklang stehen mit dem Recht der Staatsbürgerinnen und -bürger, über die Tätigkeiten der gewählten Kandidatinnen und Kandidaten und Körperschaften informiert zu werden;

in Erwägung, dass in diesem Rahmen von politischen Organisationen fortlaufend eine große Menge von Personendaten gesammelt und manchmal in aggressiver Art und Weise verwendet werden, unter Anwendung verschiedener Techniken wie Umfragen, Sammlung von E-Mail-Adressen mittels geeigneter Software oder Suchmaschinen, flächendeckender Stimmenwerbung in Städten oder Formen politischer Entscheidbildung durch interaktives Fernsehen oder Computerdateien, die die Herausfilterung einzelner Stimmenden erlauben; in Erwägung, dass in diesen Daten – zusätzlich zu elektronischen Adressen, Telefonnummern, E-Mail-Konten, Informationen über berufliche Tätigkeiten und familiäre Verhältnisse – zuweilen unrechtmäßig – auch sensible Daten enthalten sein können wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten;

in Erwägung, dass von verschiedenen Personen invasive Profile erstellt und sie klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen, ihr angehören oder gar Parteimitglieder sind, um so mit bestimmten Gruppen von Bürgerinnen und Bürgern vermehrt persönlich kommunizieren zu können;

in Erwägung, dass diese Aktivitäten gesetzeskonform und ordnungsgemäß ausgeübt werden müssen;

in Erwägung, dass es nötig ist, die Grundrechte und Grundfreiheiten der betroffenen Personen zu schützen und mit geeigneten Maßnahmen zu verhindern, dass diese Personen ungerechtfertigtes Eindringen in ihre Privatsphäre erfahren, Schaden erleiden oder ihnen Kosten entstehen, dass sie namentlich negative Auswirkungen und mögliche Diskriminierungen erleiden oder auf die Ausübung bestimmter Formen der politischen Beteiligung verzichten müssen;

in Erwägung, dass es möglich sein sollte, das Schutzziel zu erreichen, indem sowohl die Interessen der Öffentlichkeit an bestimmten Formen politischer Kommunikation als auch angemessene Modalitäten und Garantien in Bezug auf die Kommunikation mit Parteimitgliedern und mit andern Bürgerinnen und Bürgern in Betracht gezogen werden;

in Erwägung, dass in diesem Sinne ein verantwortungsbewusstes Marketing gefördert werden kann, ohne dass der Austausch politischer Ideen und Vorschläge behindert zu werden braucht, und dass die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten hat, die sie vom kommerziellen Marketing unterscheiden;

in Erwägung, dass Datenschutzgesetze bereits in vielen Gerichtsbarkeiten auf politische Kommunikation anwendbar sind;

in Erwägung, dass es nötig ist, die Einhaltung der Datenschutzesgrundsätze zu garantieren und dazu einen weltweiten Minimalstandard zu schaffen, der dazu beitragen könnte, dass das Schutzniveau für Personen, von denen Daten gesammelt werden können, zu harmonisieren, indem zum einen nationale und internationale Verhaltensregeln zur Grundlage genommen und zum anderen spezifische Lösungen und Regelungen einzelner Länder berücksichtigt werden;

in Erwägung, dass die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen könnten, auch in Zusammenarbeit mit anderen Aufsichtsbehörden in den Bereichen des Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren;

verabschiedet folgende Resolution:

Jede Aktivität politischer Kommunikation, die die Verarbeitung von Personendaten voraussetzt – auch diejenige, die nicht im Zusammenhang mit Wahlkampagnen steht – muss die Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen respektieren, einschliesslich des Rechts auf Schutz der persönlichen Daten, und muss im Einklang stehen mit den anerkannten Grundsätzen des Datenschutzes, namentlich:

Datenminimierung

Personendaten sollen nur so weit verarbeitet werden, als es zur Erreichung des spezifischen Zwecks, zu welchem sie gesammelt werden, erforderlich ist.

Erhebung auf rechtmäßige Weise und nach Treu und Glauben

Personendaten sollen aus erkennbaren Quellen rechtmäßig erhoben werden und sie sollen nach Treu und Glauben verarbeitet werden. Es soll sichergestellt werden, dass die Quellen, im Einklang mit dem Gesetz, entweder öffentlich zugänglich sind, oder dass andernfalls respektiert wird, dass sie nur zu bestimmten Zwecken, unter bestimmten Modalitäten, für einen begrenzten Anlass oder Zeitraum genutzt werden dürfen.

Besondere Aufmerksamkeit soll jenen Fällen geschenkt werden, in denen aggressive Methoden für die Kontaktaufnahme mit den betroffenen Personen gewählt werden.

Datenqualität

Bei der Verarbeitung sollen die anderen Grundsätze zur Sicherung der Datenqualität beachtet werden. Die Daten müssen insbesondere richtig, relevant und auf das notwendige Minimum beschränkt sein und à jour gehalten werden im Hinblick auf den bestimmten Zweck, zu dem sie erhoben wurden, besonders wenn sich die Informationen auf gesellschaftliche oder politische Anschauungen oder ethische Überzeugungen der betroffenen Person beziehen.

Zweckmäßigkeit

Personendaten aus privaten oder öffentlichen Informationsquellen, Institutionen oder Organisationen dürfen für die politische Kommunikation verwendet werden, wenn ihre Weiterverarbeitung im Einklang steht mit dem Zweck, zu dem sie ursprünglich erhoben wurden, und den betroffenen Personen zur Kenntnis gebracht wird; dies gilt insbesondere für sensible Daten. Gewählte Abgeordnete müssen diese Grundsätze beachten, wenn sie Daten, die zur Ausübung der amtlichen Funktionen gesammelt wurden, für die politische Kommunikation benützen wollen.

Personendaten, die ursprünglich mit aufgeklärter Einwilligung der betroffenen Person zu Marketingzwecken erhoben wurden, dürfen für die politische Kommunikation verwendet werden, wenn der Zweck der politischen Kommunikation in der Zustimmungserklärung ausdrücklich genannt wird.

Verhältnismäßigkeit

Personendaten dürfen nur auf die Art und Weise verarbeitet werden, die dem Zweck der Datensammlung entspricht, insbesondere wenn es um Daten zu potentiellen Wählerinnen und Wählern oder um den Vergleich von Daten geht, die aus verschiedenen Archiven oder Datenbanken stammen.

Personendaten, insbesondere solche, die über den Anlass hinaus, zu dem sie erhoben wurden, aufbewahrt werden, dürfen weiter verwendet werden, bis die Ziele der politischen Kommunikation erreicht sind.

Information der betroffenen Person

Den betroffenen Personen muss eine dem gewählten Kommunikationsmittel entsprechende Informationsnotiz zugestellt werden, bevor von ihnen Daten gesammelt werden; die Notiz hat den für die Datensammlung Verantwortlichen zu bezeichnen (die einzelne kandidierende Person, den externen Kampagnenleiter, die lokale Unterstützungsgruppe, lokale oder assoziierte Vereinigungen, die Partei insgesamt) sowie den zu erwartenden Datenaustausch zwischen diesen Instanzen.

Die Person, von der Daten gesammelt werden, muss informiert werden, wenn diese Daten ohne ihr Zutun gesammelt werden, zumindest wenn die Daten nicht nur vorübergehend aufbewahrt werden.

Einwilligung

Es muss sichergestellt sein, dass die Verarbeitung von Personendaten auf der Einwilligung der betroffenen Person oder auf einem anderen gesetzlich vorgesehenen Grund beruht. Die Verarbeitung muss die im jeweiligen Staat geltenden, den spezifischen Informationsquellen und -mitteln entsprechenden Regelungen beachten, namentlich im Falle von E-Mail-Adressen, Faxnummern, SMS oder andern Text/Bild/Video-Mitteilungen oder von aufgezeichneten Telefonkontakten.

Datenaufbewahrung und Datensicherheitsmaßnahmen

Jede für eine Datensammlung verantwortliche Person, sei es eine politische Gruppierung oder eine einzelne kandidierende Person, muss alle technischen und organisatorischen Massnahmen treffen, die nötig sind, um die Integrität der Daten zu schützen und um zu verhindern, dass die Daten verloren gehen oder von unbefugten Personen oder Stellen benutzt werden.

Rechte der betroffenen Person

Die betroffene Person hat das Recht auf Zugang, Berichtigung, Sperrung und Löschung ihrer Daten; sie hat das Recht, sich gegen unerwünschte Kommunikation zu wehren und – kostenlos sowie auf einfache Weise – zu verlangen, keine neuen Mitteilungen mehr zu erhalten. Diese Rechte müssen in der an sie gerichteten Informationsnotiz ausdrücklich genannt werden.

Für den Fall, dass diese Rechte verletzt werden, sind angemessene Maßnahmen und Sanktionen vorzusehen.