LANDTAG RHEINLAND-PFALZ
14. Wahlperiode

Drucksache 14/2627
05. 11. 2003

U n t e r r i c h t u n g

durch den Landesbeauftragten für den Datenschutz

Neunzehnter Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 2001 bis 30. September 2003

I n h a l t s v e r z e i c h n i s

Dem Präsidenten des Landtags mit Schreiben vom 5. November 2003 zugeleitet. Der Bericht wurde von der Kommission beim Landesbeauftragten für den Datenschutz nach § 26 Abs. 3 Satz 4 Landesdatenschutzgesetz vorberaten.

Druck: Landtag Rheinland-Pfalz, 16. Dezember 2003

Seite

Seite

Seite

Seite

Anlagen

Seite

Abkürzungen

ABl.	Amtsblatt der Europäischen Gemeinschaften
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ArbGG	Arbeitsgerichtsgesetz
ArbzG	Arbeitszeitgesetz
AuslG	Ausländergesetz
BDSG	Bundesdatenschutzgesetz
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
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
EWOIS	Einwohnerinformationssystem
FahrlG	Fahrlehrergesetz
FeV	Fahrerlaubnis-Verordnung
ff.	(fort-)folgende
FGO	Finanzgerichtsordnung
FM	Ministerium der Finanzen
FÜV	Fernmeldeüberwachungsverordnung
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
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LArchG	Landesarchivgesetz
LBG	Landesbeamtengesetz
LDI	Landesbetrieb Daten und Information
LDKN	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
lit.	littera (Buchstabe)
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LPersVG	Landespersonalvertretungsgesetz
LRG	Landesrundfunkgesetz
LSG	Landessozialgericht
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
MDK	Medizinischer Dienst der Krankenversicherung
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
MRRG	Melderechtsrahmengesetz

n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
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
PStG	Personenstandsgesetz
RdNr.	Randnummer
RDV	Recht der Datenverarbeitung
SchulG	Schulgesetz
SDÜ	Schengener Durchführungsübereinkommen
SGB I	Sozialgesetzbuch – Erstes 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
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
ZPO	Zivilprozessordnung

Glossar technischer Begriffe

ActiveX	Eine Software-Technologie von Microsoft. ActiveX erlaubt es, so genannte 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 dem 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 elektronische Signatur realisieren. Wird dabei mit dem geheimen Schlüssel des Absenders signiert, kann die Signatur anhand des öffentlichen Schlüssels 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-Attack	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-Attack 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 Protocol. 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	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 Auftragsnehmers 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 dient 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*, stellt sicher, 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 Resource Locator) angegeben. Eine typische Internet-Adresse ist z. B. http//: www.datenschutz.rlp.de.
IP-Adresse	Internet Protocol-Adresse. Nummerische 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 voreingestellten Parametern 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 konzentriert sind.
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 Test der Möglichkeiten, von außen mit den einem Angreifer verfügbaren Mitteln in ein geschütztes Netz einzudringen.

PGP	Pretty Good Privacy. Ein weitverbreitetes Programm zur Verschlüsselung und elektronischen 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 *geheimem Schlüssel*. Bei der digitalen Signatur wird durch den Absender mit dessen geheimem 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. Stattdessen 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 Internets.
RSA	Aus den Anfangsbuchstaben der Erfinder (Rivest, Shamir und Adleman) zusammengesetzte Bezeichnung für ein *asymmetrisches Verschlüsselungsverfahren*.

Schlüssellänge	Angabe über die Länge kryptografischer Schlüssel in Bit. Grundsätzlich gilt: Je länger ein Schlüssel, desto größer ist die Zahl der möglichen Ausprägungen und desto höher der Aufwand zu seiner Kompromittierung.
Schlüsselpaar	Das Paar aus geheimem und öffentlichem Schlüssel bei *asymmetrischen Verschlüsselungsverfahren*.
Server	Zentraler Rechner in einem Netzwerk, der den Arbeitsstationen/Clients Daten, Dienste usw. zur Verfügung stellt. Auf dem Server ist das Netzwerk-Betriebssystem installiert, und vom Server wird das Netzwerk verwaltet. Als Server werden neben Rechnern auch Softwarekomponenten bezeichnet, die *Client*-Prozessen, z. B. Internet-Bowsern, 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-Attack*).
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.
Subnetz	Teil eines Kommunikationsnetzes, der von anderen Teilen des Netzes abgegrenzt ist. Die Subnetzbildung kann logisch erfolgen, z. B. durch die Verwendung entsprechender Netzadressen oder physikalisch durch den Einsatz einer die Kommunikation steuernde Netzkomponente am Übergang des Subnetzes zum restlichen Netz.
Symmetrische Verschlüsselung	Verschlüsselungsverfahren, bei welchem im Gegensatz zu *asymmetrischen Verfahren* für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser muss damit dem Empfänger einer Nachricht auf einem zweiten sicheren Kanal zugeleitet werden.
TESTA-Netz	„Trans European Services for 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 Verwendnung verfällt die Transaktionsnummer.
Triple DES	Verfahren, bei welchem der Verschlüsselungsalgorithmus *DES* in drei aufeinander folgenden 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	*Server*dienst, in welchem Personen und Ressourcen mitsamt zugehörigen Attributen katalogisiert werden. Verzeichnisdienste werden z. B. als Adressverzeichnisse für die elektronische Post oder im Rahmen des Einsatzes von Signatur- und Verschlüsselungsverfahren für die Verwaltung von *Zertifikaten* eingesetzt.
Virtuelles Privates Netz	Logisches Netz auf physikalischen Kommunikationsverbindungen. Die *VPN*-Technologie ermöglicht es, verschiedene, die gleiche Infrastruktur 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*.
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*.
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

1. Vorbemerkung

Das Internet hat seinen Siegeszug im privaten wie im staatlich-öffentlichen Bereich fortgesetzt. Seine Technik bestimmt zunehmend die Kommunikation von Behörden untereinander sowie zwischen Behörden und Bürgern. Damit gewinnt der Bereich des technisch-organisatorischen Datenschutzes, also beispielsweise das Problem der zuverlässigen Verschlüsselung, der Möglichkeit anonymer Informationsbeschaffung sowie des Schutzes vor zerstörerischen und ausspähenden Angriffen auf diese Kommunikation, weiter an Bedeutung.

Daneben bleiben primär rechtliche Fragen zur Reichweite des Grundrechts auf Datenschutz im Verhältnis zu den Allgemeininteressen wie der Funktionsfähigkeit öffentlicher Stellen und der öffentlichen Sicherheit im Zentrum der Diskussion.

Im Berichtszeitraum gab es für den Datenschutz einige grundlegende Entwicklungen:

– Das allgemeine Datenschutzrecht des Landes, das Landesdatenschutzgesetz, wurde an die Europäische Datenschutzrichtlinie angepasst (in Anlehnung an die Neufassung des BDSG, s. BGBl. I 2003 S. 66; Landesdatenschutzgesetz i. d. F. des Änderungsgesetzes vom 8. Mai 2002, GVBl. S. 177). Dennoch sind aus der Sicht des Datenschutzes noch zahlreiche Anliegen offen (s. Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung, Tz. 2.3, Anlage 15);

– europäische Vorgaben zum Telekommunikations- und Teledienesterecht wurden geschaffen, aber noch nicht in nationales Recht umgesetzt (vgl. Tz. 19.1 und 19.2, 20.1);

– eine Reihe von höchstrichterlichen Entscheidungen stärkte den Datenschutz (BVerfG, NJW 2002, 2938 – informationelle Selbstbestimmung bei unerwünschter Parteienwerbung – und NJW 2002, 3619 – Mithören von Telefonaten durch Privatpersonen –; BGH, NJW 2003, 979 – Öffentlichkeitsarbeit eines Landesbeauftragten für den Datenschutz;

– bei staatlichen Eingriffsbefugnissen in den Datenschutz hat der Gedanke der Evaluation und der Befristung von Gesetzen Fuß gefasst (s. Regelungen im Terrorismusbekämpfungsgesetz des Bundes, Tz. 2.4; Regelungen im LVerfSchG – Tz. 6.1 – und im POG – Tz. 5.1 – sowie die Studie des Max-Planck-Instituts zur Telekommunikationsüberwachung, Anlage 27);

– es gab allerdings auch gesetzliche und sonstige staatliche Maßnahmen, die den Datenschutz eingeschränkt haben. Die Diskussion der letzten beiden Jahre war bestimmt von der Frage des erweiterten staatlichen Zugriffs auf Daten, sei es im Rahmen der Rasterfahndung, der präventiven Polizeiarbeit, bei der Verfolgung von Sozialhilfebetrügern oder der Verhinderung bzw. Ahndung von Steuerhinterziehungen.

Die Verwaltung stand und steht vor der schwierigen Aufgabe, das neue Landesdatenschutzgesetz in die Praxis umzusetzen. Dies ist ihr weitgehend gelungen. Allerdings waren auch Schwierigkeiten festzustellen; so gibt es Gemeinden, die ihre gesamte EDV einem privaten Dienstleister übertragen haben und selbst weder das technische Wissen noch die faktischen Möglichkeiten haben, ihre eigene Datenverarbeitung zu überwachen, zu steuern oder sonst unmittelbar zu beeinflussen (s. Tz. 21.3.7).

Die neuen Technologien, insbesondere auch das Internet und die Browser-Technologie, haben den Bereich der Verwaltung erobert: E-Government ist vom Schlagwort und Programm in vielen Bereichen zur Realität geworden. Die Automationsunterstützung verschiedener polizeilicher Aufgaben (POLADIS.net; INPOL-neu; Extra-net der Polizei –„RIVAR“–, s. Tz. 5.11) zeigt dies ebenso wie die Nutzung von EDV-Systemen im Bereich der Justiz (automatisiertes Grundbuch, Tz. 7.2.1) und in der Finanzverwaltung. Im Bereich der Kommunen ist die nahezu flächendeckende Einrichtung von Bürgerbüros zu nennen (vgl. 18. Tb., Tz. 18.4). Nicht immer hat das Datenschutzniveau mit der Fortentwicklung der Technik Schritt gehalten (s. den Beitrag zum Abrufverfahren auf das elektronische Grundbuch, Tz. 7.2.1).

Die sich ändernden Rahmenbedingungen erfassen auch und gerade die traditionell automationsunterstützt betriebenen Großverfahren. So haben sich einschneidende Veränderungen für das Einwohnerinformationssystem als eines der Verfahren mit zentraler Bedeutung für die Landes- und Kommunalverwaltung ergeben. Neben einer vollständigen konzeptionellen Umgestaltung ist eine weitgehende Auslagerung des Betriebs zentraler Komponenten zu einem privaten Unternehmen erfolgt. Die sich daraus ergebenden Gesichtspunkte waren Gegenstand einer intensiven Begleitung des Verfahrens durch den LfD (Tz. 21.2.5).

Bedeutsame Veränderungen fanden für die IT-Organisation der Landesverwaltung im Zusammenhang mit der Umwandlung des Daten- und Informationszentrums Rheinland-Pfalz (DIZ) in den Landesbetrieb Daten und Information (LDI) statt. Auf der Ebene des Landes ist damit die Verantwortung des Staates für zentrale DV-Dienstleistungen beibehalten worden (s. Tz. 21.2.1).

Staatliche und kommunale IT-Aufgaben wurden stärker differenziert: Kennzeichnend hierfür ist die Herauslösung der Kommunen aus dem rlp-Netz und der Aufbau eines separaten kommunalen Netzes mit in weiten Teilen auf nichtöffentliche Stellen übertragenen Betriebsaufgaben (Tz. 21.2.4). Es ist damit zu rechnen, dass in künftigen Verfahren – vergleichbar der Situation beim Einwohnermeldewesen – Verfahrenskomponenten und Betriebsaufgaben auf unterschiedliche Träger und verstärkt Aufgaben auf

Private (Outsourcing) verlagert werden. Angesichts der für die Realisierung von E-Governmentlösungen erforderlichen Vernetzung der beteiligten Stellen und Integration der Verfahren fordert der LfD zunehmend eine „Wächterfunktion“ staatlicher IT-Dienstleister wie dem LDI, um Gefährdungen des Datenschutzes und der Datensicherheit zu vermeiden (Tz. 21.2.5.6).

Die Eingaben, die sich zahlenmäßig auf dem Niveau der vergangenen Berichtszeiträume gehalten haben, konnten sehr häufig im Konsens mit allen Beteiligten erledigt werden.

Im Berichtszeitraum hat der LfD verstärkte Anstrengungen auf dem Gebiet der Öffentlichkeitsarbeit unternommen: Broschüren, Handreichungen für Behörden und ein neuer Internet-Auftritt des Landesbeauftragten sind dafür kennzeichnend. Auch die Zahl allgemeiner Bürgeranfragen zum Datenschutz hat zugenommen.

Die Schwerpunkte der Tätigkeit des LfD bildeten aber wie immer die folgenden Bereiche:

– Begleitung von Gesetzesvorhaben
– Beratung und Kontrolle bei Einführung und Betrieb automatisierter Verfahren der Verwaltung
– Bearbeitung von Eingaben.

Für die Behörde des LfD war schließlich die Ausrichtung und Leitung der Konferenzen der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2002 in Rheinland-Pfalz (im März in Mainz, im Oktober in Trier) ein herausragendes Ereignis.

Der Bericht zeigt, dass es dem LfD in den mit den öffentlichen Stellen geführten Diskussionen zwar häufig, aber nicht immer gelungen ist, seinem Anspruch gerecht zu werden, einen angemessenen Ausgleich zwischen den widerstreitenden Rechtsgütern und Interessen unter Betonung der individuellen Freiheitsrechte zu erreichen (s. auch den Ausblick in der Schlussbemerkung, Tz. 24).

2. Weiterentwicklung des Datenschutzrechts

2.1 Neuregelungen des Landesdatenschutzgesetzes

Mit Gesetz vom 8. Mai 2002 (in Kraft getreten am 18. Mai 2002) wurde das LDSG an vielen Punkten novelliert (GVBl. S. 177); insbesondere wurde es an die Datenschutzrichtlinie der Europäischen Gemeinschaft (Richtlinie 95/46/EG vom 24. Oktober 1995, ABl. EG Nr. L 281, S. 31) angepasst.

Als wesentliche Neuregelungen sind nunmehr hinzugekommen:

– Grundsatz der Datensparsamkeit und der Datenvermeidung, § 1 Abs. 3
– besonderer Schutz für „besondere Arten von personenbezogenen Daten“, § 3 Abs. 9
– Verbot der automatisierten Einzelentscheidung zu Lasten des Betroffenen, § 5 Abs. 5
– neue Datenschutzkontrollmaßnahmen (Verfügbarkeits-, Zweckbindungs-, Dokumentations- und Verarbeitungskontrolle), § 9 Abs. 2
– Vorabkontrollpflicht in besonderen Fällen, § 9 Abs. 5
– Erleichterung von Datenübermittlungen innerhalb der EG, § 17
– Recht auf Benachrichtigung in besonderen Fällen, § 18 Abs. 1
– Widerspruchsrecht in besonderen Fällen, § 19 Abs. 4
– Voraussetzungen der Videoüberwachung, § 34
– Bedingungen des Chipkarteneinsatzes, § 35.

Für die Bediensteten der öffentlichen Verwaltung in Rheinland-Pfalz stellt sich die schwierige Aufgabe, das neue Datenschutzrecht in die tägliche Verwaltungspraxis zu übertragen. Zur Erleichterung dieser Aufgabe hat der LfD zunächst den novellierten Gesetzestext in einer handlichen Ausgabe (zusammen mit dem Text des BDSG) veröffentlicht. Dem Gesetzestext ist ein Überblick vorangestellt, der die Neuregelungen erläutert, der es darüber hinaus aber auch ermöglichen soll, einen schnellen Einblick in die Gesetzessystematik zu gewinnen.

Das Anmeldeformular zum Datenschutzregister für die Verwaltungen war anzupassen.

Schließlich hat der LfD für die Anwendung der komplexen Neuregelungen zur Benachrichtigungspflicht der Betroffenen (§ 18 Abs. 1), der Vorabkontrollpflicht in besonderen Fällen (§ 9 Abs. 5) und des Verbots der automatisierten Einzelentscheidung zu Lasten des Betroffenen (§ 5 Abs. 5) „Checklisten“ für die Hand der behördlichen Datenschutzbeauftragten entwickelt (vgl. Tz. 2.2).

Die kommunalen Spitzenverbände sowie die Datenschutzbeauftragten der obersten Landesbehörden wurden darüber unterrichtet und gebeten, in ihren jeweiligen Bereichen diese Informationen zu verbreiten.

Darüber hinaus sind alle Informationen im Internet-Angebot des LfD abrufbar.

2.2 Checklisten des Landesbeauftragten für den Datenschutz zum neuen LDSG

Besonders die neu eingeführten Rechtsinstitute der Vorabkontrolle, der Benachrichtigungspflicht vor der automatisierten Speicherung bestimmter Daten und des Verbots der automatisierten Einzelentscheidung schienen aus der Sicht des LfD erläuterungsbedürftig: die Struktur dieser neuen Regelungen ist komplex; ihre Voraussetzungen, die kaskadenartig aufeinander aufbauen, und die jeweiligen Rechtsfolgen sind zwar unmittelbar aus dem Normtext ableitbar; es drängte sich aber auf, den Normanwendern – insbesondere auch den behördlichen Datenschutzbeauftragten –, die sich nicht ausschließlich und nicht täglich mit diesen Fragen beschäftigen, eine Handreichung zu geben, die ihnen die Aufgabe der Rezeption und die konkrete Anwendung der Normen erleichtern sollte. Die Form der Checkliste schien geeignet. Damit bleiben die Regelungen zwar komplex; insbesondere die Auslegung unbestimmter Rechtsbegriffe wird durch solche Checklisten nicht unmittelbar einfacher; jedenfalls wird aber erreicht, dass die richtigen Fragen an der richtigen Stelle im Prüfungsablauf gestellt werden und dass möglicherweise überflüssige Prüfungsfragen, die sich aufgrund vorrangiger Prüfpunkte erledigt haben, wegfallen.

Auf der Basis dieser Überlegungen hat der LfD drei Checklisten erstellt:

– zur Vorabkontrolle gem. § 9 Abs. 5 LDSG, Art. 20 EG-DSRL (s. Anlage 34);

– zur Benachrichtigungspflicht über die Speicherung von Daten, die ohne Kenntnis der Betroffenen erhoben worden sind gemäß § 18 Abs. 1 LDSG, Art. 11 EG-DSRL (s. Anlage 33), und

– zum Verbot der automatisierten Einzelentscheidung gem. § 5 Abs. 5 LDSG, Art. 15 EG-DSRL (s. Anlage 32).

Durch die damit detailliert vorgegebene Prüfungsabfolge wird deutlich, welchen Umfang der Anwendungsbereich der Vorschriften wirklich hat. Es ist zu hoffen, dass durch diese Vorgehensweise den Normanwendern die Scheu vor dem Umgang mit den komplexen gesetzlichen Regelungen genommen wird und diese Regelungen in den einschlägigen Fällen dann auch wirklich zum Tragen kommen.

2.3 Zweite Stufe der Novellierung des allgemeinen Datenschutzrechts

Trotz der Anpassung des allgemeinen Datenschutzrechts an die Vorgaben der Europäischen Datenschutzrichtlinie ist eine nicht geringe Zahl datenschutzrechtlicher Anliegen an den Gesetzgeber noch offen. Die Datenschutzbeauftragten des Bundes und der Länder haben diese Anliegen in einer Entschließung zusammengefasst, die in der Anlage 15 (Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung, Dresden, 27. bis 28. März 2003) abgedruckt ist.

2.4 Terrorismusbekämpfungsgesetze des Bundes

Angesichts des internationalen Terrorismus verabschiedete der Bundestag innerhalb weniger Monate ein umfangreiches Gesetzespaket mit zahlreichen Erweiterungen der Befugnisse von Sicherheits- und Ausländerbehörden (u. a. Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002 – Terrorismusbekämpfungsgesetz – BGBl. I S. 361; Gesetzentwurf der Bundes regierung mit Begründung Bundestagsdrucksache 14/7386). Folgende Neuregelungen sind aus der Sicht des LfD wesentlich:

Dem Bundesamt für Verfassungsschutz wird ausdrücklich die Befugnis eingeräumt, im Einzelfall zur Erfüllung bestimmter Aufgaben

– bei Luftfahrtunternehmen u. a. Auskünfte über Namen, die Inanspruchnahme von Transportleistungen und sonstige Umstände des Luftverkehrs

– bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen u. a. Auskünfte zu Konten, Konteninhabern und Geldbewegungen

– bei Personen und Unternehmen, die Postdienstleistungen erbringen, Namen, Anschriften, Postfächer und sonstige Umstände des Postverkehrs sowie

– bei Telekommunikations- und Teledienstunternehmen für die Vergangenheit und Zukunft

Auskünfte über Telekommunikationsverbindungsdaten und Telediensten utzungsdaten einzuholen.

Folgende völlig neue Befugnisse wurden geschaffen:

– Die Änderung des Pass- bzw. Personalausweisgesetzes lässt es zu, biometrische Merkmale von Fingern, Händen oder Gesicht in diese Ausweisdokumente aufzunehmen. Die Arten der biometrischen Merkmale, Einzelheiten dazu und zur Verschlüsselung sowie die Art der Speicherung, Verarbeitung und Nutzung sollen durch ein gesondertes Bundesgesetz geregelt werden. Hierzu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7. März 2002 eine Entschließung gefasst, in der die aus datenschutzrechtlicher Sicht einzuhaltenden Bedingungen im Einzelnen dargelegt sind (vgl. Anlage 7). Außerdem hat sie ein Positionspapier verabschiedet, in dem sie besonders auf Datenschutzanforderungen in Bezug auf technische Aspekte dieser Nutzung personenidentifizierender Merkmale eingegangen ist (vgl. Anlage 27).

– Im Bereich des Ausländerrechts soll der Informationsaustausch zwischen Sicherheitsbehörden und Ausländerbehörden bzw. Auslandsvertretungen verbessert werden. Neue identitätssichernde Maßnahmen wurden eingeführt und die Kontrolle von einreisenden Ausländern verschärft.

– Das Bundeskriminalamt kann nunmehr zur Erfüllung seiner Aufgaben als Zentralstelle Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung unmittelbar durch Anfragen bei öffentlichen oder nichtöffentlichen Stellen erheben und ist damit nicht mehr auf die vorrangige Anfrage bei den Polizeien des Bundes und der Länder angewiesen.

– Durch Änderung des Sozialgesetzbuchs ist eine Übermittlung von bestimmten Sozialdaten zur Durchführung einer Rasterfahndung zulässig.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Entstehung dieser Gesetze aufmerksam begleitet; sie verabschiedeten hierzu am 1. Oktober 2001 (vgl. 18. Tb, Anlage 32) und in der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 (s. Anlage 1) je eine Entschließung. Unter anderem durch den Einsatz der Datenschutzbeauftragten, allen voran des Bundesbeauftragten für den Datenschutz, wurden beim Erlass der Terrorismusbekämpfungsgesetze auch wesentliche Forderungen des Datenschutzes berücksichtigt:

– Die Geltung zahlreicher Änderungen ist auf fünf Jahre beschränkt, außerdem sind sie vor Ablauf dieser Frist zu evaluieren.

– Die Auskunftsrechte des Bundesamts für Verfassungsschutz wurden strengen Verfahrensvorschriften unterworfen.

– Die Einrichtung einer bundesweiten Zentraldatei für biometrische Merkmale wurde ausdrücklich gesetzlich ausgeschlossen.

– Im Rahmen einer Rasterfahndung dürfen Gesundheitsdaten von den Sozialbehörden nicht an die Polizei übermittelt werden.

– Dem Bundeskriminalamt wurde nicht die Befugnis eingeräumt, Vorermittlungen ohne Anfangsverdacht im Sinne der Strafprozessordnung durchzuführen.

Der BfD hat den Werdegang dieser Gesetze und die datenschutzrechtlichen Positionen hierzu in seinem 19. Tb., Tz. 2, ausführlich dargestellt.

Das (rückwirkend) am 1. Januar 2002 in Kraft getretene Gesetzespaket stellt aus der Sicht des LfD eine hinnehmbare Kompromisslösung dar. Zu begrüßen ist in erster Linie die Evaluierung und Befristung der neuen Befugnisse der Sicherheitsbehörden. Erstmals wurden – mit Vorbildwirkung für die Länder, vgl. die entsprechenden Regelungen für das Landesverfassungsschutzgesetz (Tz. 6.1) und im Entwurf des Polizeigesetzes des Landes (Tz. 5.1) – die Voraussetzungen für eine Erfolgskontrolle und die Verpflichtung zur Evaluierung im Sicherheitsbereich gesetzlich geregelt (Artikel 22 Abs. 3). Die entsprechenden Maßnahmen müssen sich als erforderlich, geeignet und verhältnismäßig erweisen. Dies ist im Rahmen der Evaluierung auf der Grundlage aussagekräftiger Berichte der jeweils zuständigen Behörden zu prüfen, d. h. die gesammelten Erfahrungen müssen gründlich ausgewertet werden. Die vor allem in präventiver Hinsicht bedeutsamen Maßnahmen im Terrorismusbekämpfungsgesetz haben sich einer kritischen Begleitung zu stellen. Dies sollte durch die lückenlose Kontrollfunktion der G 10-Kommission, des Parlamentarischen Kontrollgremiums und der Datenschutzbeauftragten sowie durch die nunmehr gesetzlich geregelte Berichts- und Evaluierungspflicht möglich sein. Es bleibt abzuwarten, wie die neuen Befugnisnormen greifen.

3. Europa

3.1 Erster Bericht der Europäischen Kommission über die Durchführung der Datenschutzrichtlinie (EG 95/46)

Die Entstehungsgeschichte und die vielschichtigen Probleme bei der Umsetzung der EG-Datenschutzrichtlinie hat der LfD in den zurückliegenden Tätigkeitsberichten dargestellt (vgl. zuletzt 18. Tb., Tz. 3.1). Nach Art. 33 der Richtlinie soll die Europäische Kommission regelmäßig über die Umsetzung der Richtlinie den Mitgliedstaaten berichten. Am 15. Mai 2003 hat die Kommission dem Europäischen Parlament und dem Rat nun erstmals einen Bericht über die Durchführung der EG-Datenschutzrichtlinie vorgelegt.

Der Kommissionsbericht kommt zu dem Ergebnis, dass die mit der Richtlinie im Jahre 1995 verfolgten Ziele der Gewährleistung eines wirksamen Datenschutzes und der Erleichterung des Austausches personenbezogener Daten innerhalb der EU im Großen und Ganzen erreicht worden seien. Die grundrechtliche Dimension der Richtlinie habe durch die Verankerung des „Rechts auf Datenschutz“ in Art. 8 der Charta der Grundrechte der Europäischen Union eine größere Bedeutung erhalten (vgl. dazu auch Tz. 3.2). Die Richtlinie selbst weise einen der höchsten Datenschutzstandards weltweit auf. Eine Änderung der Richtlinie sei daher gegenwärtig nicht erforderlich.

Aufgrund der recht unterschiedlichen Umsetzung der Richtlinie in den Mitgliedstaaten – nach Art. 249 Abs. 3 EG-Vertrag ist eine Richtlinie nur hinsichtlich ihres allgemeinen Ziels verbindlich, wohingegen die konkrete Art und Weise der Implementierung den Mitgliedstaaten selbst überlassen ist und ihnen somit ein Handlungsspielraum verbleibt – hat die Kommission erhebliche Abweichungen zwischen den Rechtsvorschriften der einzelnen Mitgliedstaaten und der Form ihrer praktischen Anwendung festgestellt. Die Unterschiede des Datenschutzrechts in den Mitgliedstaaten seien nach wie vor zu groß.

In diesem Zusammenhang ist auf eine Entscheidung des EuGH hinzuweisen, der wenige Tage nach Vorlage des Kommissionsberichts entschieden hat, dass jedenfalls die Art. 6 Abs. 1 c und 7 c und e der Richtlinie in dem Sinne unmittelbar anwendbar seien, dass sich ein Einzelner vor den nationalen Gerichten auf sie berufen kann, um die Anwendung entgegenstehender Vorschriften des innerstaatlichen Rechts zu verhindern (vgl. Urteil des EuGH vom 20. Mai 2003; C – 465/00 und C – 139/01). Die genannten Vorschriften enthalten Regelungen zu den Grundsätzen der Zweckbindung und der Erforderlichkeit bei der Erhebung und Verarbeitung personenbezogener Daten. Die Nichtumsetzung oder fehlerhafte Umsetzung der Datenschutzrichtlinie durch die Mitgliedstaaten hindert den Einzelnen also nicht daran, sich auf einzelne Bestimmungen der Richtlinie zu berufen.

Der Bericht der Kommission enthält ein Arbeitsprogramm, das dazu dienen soll, die Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten abzubauen. Bis Ende 2004 soll dieses Aktionsprogramm abgeschlossen sein, als dessen Grundlage der Dialog zwischen der Kommission und den Mitgliedstaaten und die Zusammenarbeit der nationalen Datenschutzbehörden, insbesondere im Rahmen der nach Art. 29 der Richtlinie geschaffenen Datenschutzgruppe, dient. In dem für das Jahr 2005 vorgesehenen Folgebericht wird die Kommission das Ergebnis des Arbeitsprogramms prüfen und entscheiden, ob Vorschläge zur Änderung der Datenschutzrichtlinie erforderlich sind.

3.2 Der EU-Verfassungskonvent und der Datenschutz

Im Zuge der umfassenden Reform der Europäischen Union beauftragten die europäischen Staats- und Regierungschefs am 15. Dezember 2001 einen parlamentarischen „EU-Konvent zur Zukunft Europas“ damit, die Regierungskonferenz 2004 vorzubereiten und „die wesentlichen Fragen zu prüfen, welche die zukünftige Entwicklung der Europäischen Union aufwirft“. Ein solches Konventsmodell hatte sich bereits bei der Erarbeitung der EU-Grundrechtecharta bewährt. Der Konvent selbst, der am 1. März 2002 seine Arbeit aufnahm, setzte es sich zum Ziel, nicht nur die an ihn gestellten Fragen zu beantworten, sondern einen umfassenden „europäischen Verfassungsvertrag“ auszuarbeiten. Unter dem Vorsitz des ehemaligen französischen Staatspräsidenten Valéry Giscard d’Estaing tagte der 105-köpfige Konvent, der sich hauptsächlich aus Vertretern der Regierungen der Mitgliedstaaten, Mitgliedern des Europäischen Parlaments und Vertretern der nationalen Parlamente zusammensetzte, für die Dauer von fast anderthalb Jahren. Der vollständige Entwurf des Verfassungsvertrages (im Internet unter http://european-convention.eu.int abrufbar) wurde am 18. Juli 2003 an die italienische Ratspräsidentschaft übergeben. Ziel ist es nun, die Verfassung rechtzeitig vor den im Juni 2004 stattfindenden Europawahlen zu unterzeichnen.

Für den europäischen Datenschutz ist der Verfassungsentwurf vor allem deshalb von Bedeutung, weil die Charta der Grundrechte der EU, die bisher keinen rechtsverbindlichen Status aufwies (vgl. dazu 18. Tb., Tz. 3.3), nunmehr unmittelbar in der Verfassung verankert werden soll. Nach Art. 7 Abs. 1 des Verfassungsentwurfs erkennt die Union „die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte als Teil II der Verfassung enthalten sind“. Die Grundrechtecharta wiederum enthält in Art. 8, nunmehr Art. II – 8 des Verfassungsentwurfs, das Recht des Einzelnen auf den Schutz der ihn betreffenden personenbezogenen Daten. Inhalt und Grenzen dieses „Rechts auf Datenschutz“ bestimmen sich nach den gemeinschaftsrechtlichen Regelungen, also insbesondere der EG-Datenschutzrichtlinie.

Insgesamt ist festzustellen, dass aus den Arbeiten des Verfassungskonvents die Grundrechte allgemein und damit auch das „Grundrecht auf Datenschutz“ gestärkt hervorgehen.

3.3 Die „Cyber-Crime“-Konvention des Europarates

Der Europarat hat zusammen mit Japan, Kanada, Südafrika und den USA eine Konvention über Datennetzkriminalität (Convention on Cyber-Crime) entworfen. Am 23. November 2001 unterzeichneten in Budapest, die meisten Mitgliedstaaten des Europarates, darunter auch Deutschland, und die vier beteiligten außereuropäischen Staaten die Konvention. Diese tritt jedoch erst in Kraft, wenn mindestens fünf Staaten, darunter drei Mitgliedstaaten des Europarates, sie ratifiziert haben. Derzeit (Stand: 30. September 2003) haben nur Albanien, Kroatien und Estland ratifiziert. Eine Übersicht über den jeweils gegenwärtigen Stand der Ratifizierungen und der Konventionstext sind im Internet abrufbar
htp://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185).

Über den Inhalt der Konvention und die Diskussionen im Vorfeld der Verabschiedung der Konvention wurde bereits im 18. Tb. (Tz. 3.4) berichtet.

Es ist zu bemängeln, dass einige wichtige datenschutzrechtliche Belange in der Konvention nicht ausreichend berücksichtigt worden sind. So fehlen beispielsweise materielle Bestimmungen zum Datenschutz oder zum Fernmeldegeheimnis. Auch unterliegen Rechtshilfeersuchen anderer Staaten keinerlei Einschränkungen zum Schutz der Betroffenen und es wird dem Betroffenen kein Rechtsschutz bei der Übermittlung seiner Daten garantiert. Im Übrigen ist zu befürchten, dass es hierbei zu Widersprüchen zu den Schutzstandards in der Europäischen Union und Deutschlands kommt.

3.4 Artikel 29-Datenschutzgruppe

Die Gruppe ist gemäß Art. 29 der EG-Datenschutzrichtlinie eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben wurden bereits im 18. Tb. (Tz. 3.6) näher beschrieben.

Auch während des aktuellen Berichtszeitraums wurden einige wichtige Dokumente von der Art. 29-Datenschutzgruppe angenommen (sog. Arbeitspapiere/WP). Hervorzuheben sind hierbei insbesondere:

– das Arbeitsdokument zur elektronischen Verwaltung (E-Government) vom 8. Mai 2003 (WP 73), in dem die aktuelle Situation in diesem Bereich dargestellt wird, insbesondere in Bezug auf den Schutz personenbezogener Daten von Einzelpersonen in der Europäischen Union. Hierin wird beispielsweise die weit verbreitete Möglichkeit des einheitlichen Zugangs zu Verfahren der Online-Verwaltung (sog. „Portal"-Ansatz) untersucht oder die vermehrte Tendenz der Nutzung elektronischer Ausweise;

– das Arbeitsdokument zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung vom 25. November 2002 (WP 67), in dem die datenschutzrechtlichen Anforderungen an solche Videosysteme dargestellt werden;

– das Arbeitsdokument zur Funktionsweise des Safe Harbor-Abkommens vom 2. Juli 2002 (WP 62). Im 18. Tb. (vgl. Tz. 3.5 sowie Anlage 29) wurden die Hintergründe und der Sachstand zu den Prinzipien des „Sicheren Hafens" – die der Gewährleistung eines angemessenen Datenschutzniveaus in den USA dienen – dargestellt. Eine abschließende Bewertung der Vereinbarung will die Gruppe jedoch erst nach Auswertung weiterer Informationen vornehmen. So wurden alle betroffenen Behörden, Organisationen und Verbände in der Europäischen Union aufgefordert, über bestimmte Erkenntnisse zu informieren, beispielsweise über Möglichkeiten für verfeinerte Streitbeilegungsmechanismen;

– die Stellungnahme über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen am Beispiel IPv6 vom 30. Mai 2002 (WP 58). Der Übergang zum neuen Internetprotokoll IPv6 ermöglicht es, dem einzelnen Nutzer eine eindeutige Kennung zuzuweisen. Es besteht die Gefahr, dass auf diese Weise Profile über die Internetnutzung des Einzelnen erstellt werden. Die Gruppe befürwortet es daher, technische Lösungen zu entwickeln, die dem Schutz der anfallenden Telekommunikationsdaten dienen;

– das Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten vom 29. Mai 2002 (WP 55). In diesem werden Empfehlungen gegeben zum Datenschutz bei der Überwachung des E-Mail-Verkehrs und der Kontrolle des Internetzugriffs von Arbeitnehmern.

Sämtliche Arbeitspapiere der Art. 29-Datenschutzgruppe sind im Internet unter http://europa.eu.int/comm/internal_market/privacy/workingroup_de.htm abrufbar.

4. Meldewesen

4.1 Gesetz zur Änderung des Melderechtsrahmengesetzes

Den Gesetzentwurf hat der LfD im 18. Tb., Tz. 4.2 im Einzelnen dargestellt. Am 3. April 2002 ist das Gesetz zur Änderung des Melderechtsrahmengesetzes vom 25. März 2002 in Kraft getreten (BGBl. I S. 1186). Mit den Änderungen sollen die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien geschaffen werden. Aus datenschutzrechtlicher Sicht sind insbesondere folgende Neuregelungen von Bedeutung:

§ 8 MRRG regelt die Auskunft an den Betroffenen. Nach der Neuregelung in Abs. 2 kann die Auskunft nach näherer Maßgabe des Landesrechts auch im Wege des automatisierten Abrufs über das Internet erteilt werden. Dabei ist zu gewährleisten, dass dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten. Der Nachweis der Urheberschaft des Antrags ist durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu führen. Die Vertraulichkeit der Daten ist durch die Verschlüsselung der Auskunft sicherzustellen. Zu den Anforderungen an Form und Inhalt des Antrags verweist § 8 Abs. 2 MRRG auf § 21 Abs. 1 a Satz 1 MRRG, der die Zulässigkeit der einfachen Melderegisterauskunft mittels des elektronischen Verfahrens regelt.

§ 11 Abs. 6 MRRG ermöglicht es den Ländern, die elektronische Anmeldung zuzulassen. Durch einen Verweis auf § 8 Abs. 2 MRRG werden die Meldebehörden zu den dem jeweiligen Stand der Technik entsprechenden Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit verpflichtet.

§ 21 Abs. 1 a MRRG regelt die Zulässigkeit der Erteilung einer einfachen Melderegisterauskunft auf automatisiert verarbeitbaren Datenträgern, durch Datenübertragung oder im Wege des automatisierten Abrufs über das Internet. Einem automatisierten Abruf über das Internet kann der Betroffene widersprechen.

Die Länder haben ihr Melderecht innerhalb von zwei Jahren nach In-Kraft-Treten dieses Gesetzes anzupassen.

Verschiedene Forderungen der Datenschutzbeauftragten (vgl. die Entschließung vom 9. März 2001, 18. Tb., Anlage 24) sind jedoch nicht berücksichtigt worden. So wurde die Hotelmeldepflicht nicht abgeschafft. Weiter wurde die einfache Melderegisterauskunft über das Internet nicht von der ausdrücklichen Einwilligung des Betroffenen abhängig gemacht. In diesen Fällen wurde jedoch

zumindest ein Widerspruchsrecht geschaffen. Des Weiteren dürfen auch künftig Melderegisterauskünfte an politische Parteien zu Wahlwerbezwecken erteilt werden, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Da die Widerspruchslösung in weiten Kreisen der Bevölkerung unbekannt ist, hatten die Datenschutzbeauftragten eine Einwilligungsregelung gefordert.

4.2 Die Auskunftssperren

Den LfD erreichen häufig Anfragen im Hinblick auf melderechtliche Auskunftssperren. Mit dem Ziel, dem Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung Geltung zu verschaffen, hat der Gesetzgeber die Einrichtung folgender Auskunftssperren zugelassen:

- Sperrung jeglicher Datenübermittlung, wenn Tatsachen die Annahme rechtfertigen, dass den Betroffenen oder anderen Personen hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen können (§ 34 Abs. 7 i. V. m. Abs. 5 MG)
- Sperrung der Datenübermittlung im Rahmen einer erweiterten Melderegisterauskunft oder einer Gruppenauskunft (§ 34 Abs. 7 i. V. m. Abs. 6 MG)
- Sperrung der Übermittlung der Meldedaten von Familienangehörigen, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgemeinschaft angehören (§ 32 Abs. 2 MG)
- Sperrung der Datenübermittlung an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlaments-, Kommunal- und Ausländerbeiratswahlen (§ 35 Abs. 1 MG)
- Sperrung der Datenübermittlung zu Gratulationszwecken (§ 35 Abs. 2 MG)
- Sperrung der Datenübermittlung an Adressbuchverlage (§ 35 Abs. 4 MG).

Die unterschiedlichen Auskunftssperren müssen jeweils beantragt werden. Lediglich die Auskunftssperre nach § 34 Abs. 5 MG ist nicht nur auf Antrag, sondern auch von Amts wegen einzutragen, wenn eine der im Gesetz beschriebenen Gefährdungen vorliegt.

Für einen Minderjährigen ist grundsätzlich der gesetzliche Vertreter antragsberechtigt. Hier sind aber auch melderechtliche Besonderheiten zu beachten: Was z. B. die Datenübermittlung an Adressbuchverlage anbelangt, könnte hinsichtlich einer Auskunftssperre für Minderjährige auf § 35 Abs. 4 MG verwiesen werden. Diese Norm besagt jedoch lediglich, dass an Andressbuchverlage eine einfache Melderegisterauskunft über sämtliche Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden darf, sofern die Betroffenen nicht widersprochen haben. Die vorherige Ausübung des Grundrechts auf informationelle Selbstbestimmung ist nach Auffassung des LfD hierdurch nicht ausgeschlossen. Es sollten daher auch Widersprüche beachtet werden, die von Jugendlichen im Hinblick auf die Vollendung ihres 18. Geburtstages eingelegt werden. Die mögliche Sperrung der Datenübermittlung im Bereich der Wahlwerbung (vgl. § 35 Abs. 1 MG) sollte entsprechend behandelt werden.

4.3 Erteilung einer Gruppenauskunft an das Deutsche Rote Kreuz (DRK)

Eine Verbandsgemeindeverwaltung schilderte dem LfD das Interesse des DRK, aus dem Datenbestand des Melderegisters im Rahmen der Nachwuchsarbeit die Adressen aller weiblichen und männlichen Personen im Alter zwischen 20 und 30 Jahren zu erhalten. Sie bat zu prüfen, ob die entsprechende Melderegisterauskunft zulässig ist.

Die Gruppenauskunft ist bereichsspezifisch im Meldegesetz geregelt. Als Rechtsgrundlage kommt sowohl § 31 Abs. 1 als auch § 34 Abs. 3 MG in Betracht. Nach § 31 Abs.1 MG darf die Meldebehörde einer sonstigen öffentlichen Stelle 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. Bei dem DRK handelt es sich indessen um eine nicht öffentliche Stelle, so dass eine Übermittlung nach § 31 Abs. 1 MG ausscheidet. Gem. § 34 Abs. 3 MG sind Gruppenauskünfte zulässig, wenn sie im öffentlichen Interesse liegen. Nach Nr. 16.3 der Verwaltungsvorschrift zur Durchführung des Meldegesetzes vom 19. Februar 1999 (MinBl. S. 203) ist das öffentliche Interesse für eine Gruppenauskunft in der Regel anzunehmen u. a. bei Auskunftsersuchen der Spitzenverbände der freien Wohlfahrtspflege und der ihnen angeschlossenen Verbände zum Zwecke der Betreuung alter Menschen, Jugendlicher und sonstiger Betreuungsgruppen. Das Anliegen des DRK, im vorliegenden Fall die Nachwuchsarbeit, dürfte auch ohne persönliche Ansprache Betroffener im Wege der Öffentlichkeitsarbeit (z. B. Schaltung von Zeitungsannoncen) realisiert werden können. Hinzu kommt, dass anderenfalls dann wohl auch Konkurrenzorganisationen (z. B. „Malteser“, „ASB“) mit dem gleichen Ansinnen an das Meldeamt herantreten würden, um Wettbewerbsnachteile zu vermeiden. Hier wird deutlich, dass es sich vorliegend nicht um ein öffentliches Interesse im Sinne von § 34 Abs. 3 MG handelt. Mithin kam aus Sicht des LfD die in Rede stehende Datenübermittlung nicht in Betracht. In diesem Zusammenhang wies er auf Folgendes hin: Ein datenschutzverträglicher Weg könnte darin bestehen, dass die kuvertierten und frankierten – und lediglich „adresslosen“ – Anschreiben des DRK direkt vom Meldeamt mit Adressaufklebern versehen und an die Betroffenen verschickt werden. Im Wege dieser so genannten „Datenmittlung“ ergibt sich kein datenschutzrechtliches Problem: Hier erfolgt nämlich keine Übermittlung personenbezogener Daten an das DRK. Eine entsprechende Information der Zielgruppe wäre aber dennoch gewährleistet. So werden auf diese Art und Weise die Betroffenen in die Lage versetzt, selbst über eine mögliche Kontaktaufnahme mit dem DRK zu entscheiden.

4.4 Gruppenauskünfte an gesetzliche Krankenkassen und private Krankenversicherer?

Den LfD erreichten seitens einiger Verbandsgemeindeverwaltungen Anfragen, in denen es um das dargelegte Interesse von Krankenkassen bzw. privaten Krankenversicherungen ging, aus dem Datenbestand des Melderegisters die Adressen jener Haushalte der Verbandsgemeinde zu erhalten, in denen als Zielgruppe für die Versichertenwerbung Jugendliche eines bestimmten Alters leben.

Die Meldebehörde darf nach § 31 Abs. 1 MG einer sonstigen öffentlichen Stelle – hier einer gesetzlichen Krankenkasse als Körperschaft des öffentlichen Rechts (§ 4 SGB V) – aus dem Melderegister bestimmte Daten übermitteln, wenn dies zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Nach Auffassung des LfD bestehen vorliegend Bedenken hinsichtlich der Erforderlichkeit der Übermittlung der angeforderten Meldedaten. Insoweit dürfte ein entsprechender gesetzlicher Auftrag auch ohne persönliche Ansprache Betroffener im Wege der Öffentlichkeitsarbeit oder in sonstiger Form realisiert werden können. Soweit das Auskunftsersuchen von gesetzlichen Krankenkassen an die Meldebehörden zu dem Zweck erfolgt, die Angehörigen einer bestimmten Zielgruppe zu bewerben, sind außerdem die für private Krankenversicherer entstehenden Wettbewerbsnachteile zu berücksichtigen, da insoweit ein öffentliches Interesse an einer Gruppenauskunft nicht anzuerkennen ist. So begründen die Durchführung von Werbemaßnahmen für einzelne Produkte oder sonstige kommerzielle Interessen – dazu gehört aus Sicht des LfD auch die Mitgliederwerbung – regelmäßig kein öffentliches Interesse im Sinne des § 34 Abs. 3 MG.

Mithin kam nach Auffassung des LfD die in Rede stehende Datenübermittlung nicht in Betracht.

4.5 Durchführung wissenschaftlicher Erhebungen mittels Gruppenauskunft aus dem Melderegister

Behördliche Anfragen zu den von Forschungseinrichtungen begehrten Datenübermittlungen offenbarten immer wieder Probleme bei der Anwendung der Vorschriften zur Gruppenauskunft. Aufgrund der oftmals herrschenden Unklarheiten zu diesem Thema hat der LfD in einer Handreichung – die auch in sein Internetangebot unter „Aktuelles“ aufgenommen wurde – darauf hingewiesen, dass als Rechtsgrundlage für die Gruppenauskunft § 34 Abs. 3 MG mit dem dort beschriebenen Datensatz in Betracht kommt. Danach sind Gruppenauskünfte zulässig, wenn sie im öffentlichen Interesse liegen. Nach Nr. 16.3 der Verwaltungsvorschrift zur Durchführung des Meldegesetzes vom 19. Februar 1999 (MinBl. S. 203) ist das öffentliche Interesse für eine Gruppenauskunft in der Regel anzunehmen u. a. für Datenübermittlungen zum Zwecke der wissenschaftlichen Forschung. Des Weiteren sind danach Gruppenauskünfte in der Regel mit folgenden Hinweisen zu versehen: „Beabsichtigen die Antragsteller (z. B. Forschungsinstitute) die von der Gruppenauskunft Betroffenen zu befragen oder um Teilnahme an bestimmten Vorhaben zu bitten, so sind die Betroffenen darauf hinzuweisen, dass die Beantwortung der Fragen und die Teilnahme an der Erhebung freiwillig sind. Erfolgt der Hinweis zusammen mit anderen Erklärungen, so ist er deutlich hervorzuheben. Die Betroffenen sind über den Inhalt und den Zweck der Befragung oder des Vorhabens sowie über die Auswertung und die weitere Verwendung der Daten zu informieren. Daten von Personen, die die Beantwortung der Fragen oder die Teilnahme an dem Vorhaben verweigern, sind unverzüglich zu löschen. Die Daten dürfen nur für das Projekt verwendet werden, für das sie übermittelt wurden; sie sind gegen unberechtigte Zugriffe zu sichern und nach Abschluss des Projekts unverzüglich zu löschen. Zusammenstellungen über Ergebnisse dürfen keine Angaben enthalten, die auf bestimmte oder bestimmbare Personen hinweisen.“

Von besonderer Bedeutung ist stets, dass etwa vorhandene Auskunftssperren für Gruppenauskünfte (vgl. § 34 Abs. 6 MG) zu berücksichtigen sind. Werden Angaben zur Staatsangehörigkeit erbeten, ist die Regelung in § 34 Abs. 3 Satz 4 MG zu beachten, wonach eine Gruppenauskunft, die das Datum Staatsangehörigkeit enthält, nur mit Zustimmung des fachlich zuständigen Ministeriums (hier: Ministerium des Innern und für Sport) erteilt werden darf.

Was die Ausgestaltung des Schreibens der jeweiligen Forschungseinrichtung an die potentiellen Teilnehmer anbelangt, sollte seitens der Meldeämter angeregt werden, folgende Formulierung bezüglich der Herkunft der Adressen zu verwenden: „Ihre Adresse wurde uns im Wege einer sog. Gruppenauskunft von ... (Bezeichnung der Kommune) zur Durchführung des beschriebenen, im öffentlichen Interesse liegenden Forschungsvorhabens mitgeteilt.“

Schließlich ist zu bedenken, dass auch im Falle einer zulässigen Gruppenauskunft ein Anspruch auf die entsprechende Datenübermittlung unter Beachtung des Gleichheitssatzes nicht ableitbar ist.

5. Polizeibereich; Vorbemerkung

Die aufgrund des 11. September 2001 eingeleiteten Gesetzesänderungen auf der Ebene des Bundes wurden oben unter Tz. 2.4 bereits dargestellt. Auf der Ebene des Landes sind u. a. die Rasterfahndung nach „Schläfern“ (Tz. 5.2) und die vorgesehene Novellierung des Polizei- und Ordnungsbehördengesetzes (Tz. 5.1) Folgen der neuen Gefährdungssituation.

Im Sicherheitsbereich gab und gibt es aber auch Entwicklungen, die das Datenschutzgrundrecht stärken. Nicht zuletzt die Verfassungsrechtsprechung gibt immer wieder Impulse, die Praxis der Sicherheitsbehörden kritisch zu überprüfen und einzelne Verbesserungen im Sinne des Datenschutzes anzumahnen. Dazu gehört auch die Forderung, solche Daten bei den Behörden gesondert zu kennzeichnen, die aus heimlichen oder aus sonstigen Gründen als besonders eingreifend anzusehenden Datenerhebungen stammen. Die Kennzeichnung soll ermöglichen, dass die speichernden Stellen mit diesen Daten so umgehen, wie es ihre Sensibilität erfordert; insbesondere ist auf die Einhaltung der Zweckbindung bei der Verwendung dieser Daten besonders zu achten (s. dazu die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2002, „Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen“, Anlage 19).

5.1 Novellierung des Polizei- und Ordnungsbehördengesetzes

Die Landesregierung verfolgt das Ziel, durch eine umfassende Novellierung des POG ein „modernes Polizeirecht“ zu schaffen. Nach der Begründung zum Gesetzentwurf (Landtagsdrucksache 14/2287 vom 24. Juni 2003) sollen der Polizei die „für die Gewährleistung der inneren Sicherheit erforderlichen Befugnisse“ zur Verfügung gestellt werden. Eine Fortentwicklung des materiellen Polizeirechts sei vor allem für die Bekämpfung der unterschiedlichsten Erscheinungsformen der organisierten Kriminalität und die Gewährleistung eines wirkungsvollen Schutzes der Bevölkerung vor terroristischen Anschlägen erforderlich.

Durch den vorliegenden Gesetzentwurf würden insbesondere die Befugnisse der allgemeinen Ordnungsbehörden und der Polizei „den aktuellen Bedürfnissen“ angepasst, „um zukünftigen Anforderungen in vollem Umfang gerecht werden“ zu können. Hierzu sollen die Befugnisse zur Informationsverarbeitung einer vollständigen Neuregelung zugeführt sowie die so genannten polizeilichen Standardmaßnahmen erweitert und ergänzt werden.

Die derzeitigen Befugnisse der Polizei zur Gefahrenabwehr würden nicht mehr ausreichen, um insbesondere den neueren Erscheinungsformen der schweren Kriminalität wie dem internationalen Terrorismus sowie den unterschiedlichsten Erscheinungsformen der organisierten Kriminalität wirksam begegnen zu können. Die Begehung dieser Straftaten hätte seit längerem gemeinsam, dass Planung, Vorbereitung und Durchführung hoch professionell, arbeitsteilig, streng abgeschottet und unter Verwendung modernster Kommunikationstechnologien erfolgen würden. Herkömmliche kriminalpolizeiliche Ermittlungsmethoden genügten zu deren Bekämpfung nicht mehr, da strafrechtliche Ermittlungen erst durchgeführt werden könnten, wenn zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen. Sie müssten von vornherein auf Klärung eines bestimmten Tatverdachts gerichtet sein. Das Gefahrenabwehrrecht müsse hingegen bereits die Entstehung solcher Gefahrenlagen verhindern. Die Polizei müsse demgemäß ihre Fahndungs- und Beobachtungsmethoden der Langfristigkeit und Weiträumigkeit der Strategien des organisierten Verbrechens anpassen, um bereits die frühe Entstehungsphase von Straftaten sowie internationale Zusammenhänge, Arbeitsweisen, kriminelle Strukturen und deren Hintermänner erkennen zu können. Hierzu sei es erforderlich, Maßnahmen zur vorbeugenden Bekämpfung von Straftaten zu treffen sowie technische Möglichkeiten wie beispielsweise die Telekommunikationsüberwachung zu nutzen.

So seien insbesondere die derzeitigen Befugnisse der Polizei zur verdeckten Informationsbeschaffung für eine erfolgreiche präventive Bekämpfung der Kriminalität nicht zufrieden stellend. Sie sollen deshalb durch den vorliegenden Gesetzentwurf erweitert und verbessert werden.

Unter anderem sollen folgende neue polizeiliche Befugnisse, die stark in die Rechte der Bürger eingreifen, eingeführt werden:

- Antwortpflicht auch von Zeugnisverweigerungsberechtigten, z. B. Ärzten und Rechtsanwälten, zur Gefahrenabwehr.
- Telekommunikationsüberwachungen zur Gefahrenabwehr.
- Einsatz von Wanzen und Video-Kameras („Großer Lausch- und Spähangriff“) in Wohnungen, mit nach jeweils drei Monaten zu erneuerndem richterlichen Beschluss zeitlich unbegrenzt, bei Gefahr im Verzug mit einer Anordnungsbefugnis des Behördenleiters.
- Rasterfahndung auch zur vorbeugenden Straftatenbekämpfung, nicht nur zur Abwehr dringender Gefahren.

Eine ganze Reihe der im Entwurf enthaltenen Änderungen kann als Präzisierung und damit Verbesserung der bestehenden Rechtslage angesehen werden. Die Argumente für die Neuregelung bzw. Erleichterung der Voraussetzungen der vorgenannten besonderen Eingriffsmittel haben den LfD aber nicht überzeugt. Er ist der Auffassung, dass die erforderliche Balance zwischen Freiheit und Sicherheit an diesen Punkten im vorliegenden Gesetzentwurf nicht erreicht wird. Im Gesetzgebungsverfahren gab es zwar verschiedene Veränderungen zugunsten des Datenschutzes. So ist die nach fünf Jahren vorgesehene Überprüfung von Wirksamkeit und Angemessenheit einiger neuer Eingriffsbefugnisse (Großer Lausch- und Spähangriff, Rasterfahndung, Sicht- und Anhaltekontrollen im öffentlichen Verkehrsraum und Telefonüberwachung zur vorbeugenden Straftatenbekämpfung) sehr zu begrüßen, und die Vorschrift über die anlasslose Personenkontrolle, jetzt „Sicht- und Anhaltekontrolle im öffentlichen Verkehrsraum“ genannt, wurde datenschutzgerecht neu gefasst. Es bleiben aber einige Bedenken bestehen.

Die Voraussetzungen für diese neuen Befugnisse bestehen aus mehrfach hintereinander gekoppelten unbestimmten Rechtsbegriffen mit unscharfen Konturen. Im Polizeirecht soll damit künftig bewusst und ausdrücklich die bisher maßgebliche spezifische polizeirechtliche Schranke für gravierende Eingriffsmaßnahmen, die konkrete Gefahr, durch Voraussetzungen ersetzt werden, die erheblich weniger konkret sind. Damit werden eingreifende Gefahrenaufklärungsmaßnahmen, die im Bereich der Strafverfolgung, im Strafprozessrecht, von einem konkreten Anfangsverdacht abhängen, im Polizeirecht unter eher diffusen Voraussetzungen möglich, die weit ins Vorfeld dieses konkreten Verdachts reichen. Eingriffe zur Gefahrenaufklärung werden sehr umfassend möglich. Der Richtervorbehalt, der nur für wenige äußerst einschneidende Eingriffe vorgesehen ist (Telekommunikationsüberwachungsmaßnahmen; Großer Lausch- und Spähangriff in Wohnungen; außerhalb von Wohnungen bei einer Dauer von mehr als sieben Tagen), ist keine sichere Schranke zur Wahrung der Verhältnismäßigkeit bei den vorgesehenen intensiven Eingriffsmaßnahmen, wenn keine weiteren Regelungen zu den Anforderungen an das Verfahren und die Begründung hinzukommen.

– Es bestehen weiterhin grundsätzliche Bedenken gegen die Verhältnismäßigkeit des „Großen Spähangriffs“. Diese Befugnis sollte entfallen. Sie droht in den unantastbaren Kernbereich des Grundrechts auf unbeobachtete Kommunikation im persönlichen Rückzugsraum der Wohnung einzugreifen.

– Die besonderen Berufsgeheimnisse im Rahmen dieser Maßnahme sowie beim „Großen Lauschangriff“ und der Telekommunikationsüberwachung zur vorbeugenden Straftatenbekämpfung sollten aus der Sicht des LfD stärker geschützt werden.

– Die neu eingeführte Befugnis der „Polizeilichen Beobachtung“ sollte nur auf der Grundlage einer richterlichen Anordnung erfolgen, die bisher hier nicht vorgesehen ist.

– Die Voraussetzungen der besonderen Eingriffsmaßnahmen sollten enger gefasst werden: Sie sollten nur dann eingesetzt werden, wenn Personen betroffen sind, bei denen bestimmte schwerwiegende Tatsachen (und nicht nur tatsächliche Anhaltspunkte) die Annahme rechtfertigen, dass sie künftig Straftaten begehen.

– Die neu eingeführte Regelung zur Video-Überwachung sollte in den Bereich der Überprüfungspflicht nach fünf Jahren einbezogen werden.

Insgesamt fehlt aus der Sicht des LfD eine überzeugende, auf konkrete Fakten gestützte Begründung für diese massive Verschärfung der gesetzlichen Eingriffsbefugnisse für die Polizei. Konkrete Fälle, in denen aufgrund des Fehlens der hier in Rede stehenden Befugnisse Defizite in der Gefahrenabwehr in Rheinland-Pfalz bestanden hätten, sind bislang nicht vorgetragen worden.

5.2 Rasterfahndung

Als Reaktion auf die Terroranschläge vom 11. September 2001 in den USA wurden bereits Ende September 2001 auch in Rheinland-Pfalz präventivpolizeiliche Fahndungsmaßnahmen (Rasterfahndung) zur Entdeckung potentieller islamistischer Terroristen und ihrer Unterstützer (Schläfer) auf der Grundlage des § 25 d Abs. 1 POG angeordnet. Nach dieser Vorschrift kann die Polizei zur Abwehr einer gegenwärtigen erheblichen Gefahr von öffentlichen und nichtöffentlichen Stellen die Übermittlung personenbezogener Informationen oder Informationsbeständen bestimmter Personengruppen auch zum Zwecke des Abgleichs mit anderen Informationsbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist. Abweichend von den Regelungen anderer Bundesländer ist in Rheinland-Pfalz der Behördenleiter gemäß § 25 d Abs. 3 POG befugt, die Rasterfahndung anzuordnen. Der LfD wurde frühzeitig in das Anordnungsverfahren eingebunden und fortlaufend über den Sachstand informiert. Der anfängliche Datenbestand von 13 000 Datensätzen reduzierte sich nach dem Abgleich mit den relevanten Datenbeständen auf ca. 1 700 Prüffälle mit Gefährderrelevanz, die im Einzelnen überprüft wurden. Umfeldermittlungen verdichteten die Prüffälle auf ca. 900. Zum überwiegenden Teil konnte die Überprüfung dieser „ausgerasterten“ Personen bereits Ende 2002 abgeschlossen werden. Die „Schläfer-Detektion“ wird voraussichtlich Mitte des vierten Quartals 2003 abgeschlossen sein. Das mit dem LfD abgestimmte Löschkonzept sieht eine Prüffrist der in der Datei zur Prüfung der Gefährderrelevanz erfassten Personen zwölf Monate nach Erfassung des Ereignisses vor. Im Zusammenhang mit der Rasterfahndung erhielt der LfD zahlreiche Anfragen hinsichtlich der Zulässigkeit der Fahndungsmaßnahme und der Auskunftsansprüche gegenüber den auskunftserteilenden Institutionen. Um Auskunft ersuchten sowohl die von der Maßnahme betroffenen Personen als auch solche Stellen, die von der Polizei zur Datenpreisgabe aufgefordert worden waren. Dass die von der Polizei durchgeführte Rasterfahndung rechtmäßig war, bestätigten auch das VG Mainz (Beschluss vom 1. Februar 2002, Az.: 1 L 1106/01) und das OVG Koblenz (Beschluss vom 27. August 2002, Az.: 12 B 11008/02).

Der Berliner Datenschutzbeauftragte hat den genauen Ablauf einer solchen Rasterfahndung mit den jeweils einbezogenen Personengruppen und Merkmalen detailliert in seinem 121 Seiten umfassenden „Sonderbericht vom 10. Dezember 2002 über die Durchführung besonderer Formen des Datenabgleichs (Rasterfahndung) durch den Polizeipräsidenten in Berlin nach dem 11. September 2001“ dargestellt. Dieser Bericht ist im Internet unter datenschutz-berlin.de/informat/sonderbericht/rasterfahndung.pdf abrufbar. Dort werden auch die jeweiligen Datei-Errichtungsanordnungen dokumentiert. Die darin zum Ausdruck kommende offene Informationspolitik der Sicherheitsbehörden des Landes Berlin ist aus Datenschutzsicht zu begrüßen.

Wie das BKA Anfang September 2003 mitteilte, wurden die Verbunddatei „Schläfer“ und damit die Grunddatenbestände der Länder sowie die Abgleichdateien am 30. Juni 2003 gelöscht bzw. vernichtet.

5.3 Ein neues Telekommunikations-Überwachungs-System

Die herkömmliche Technik der analogen Aufzeichnung von Telefongesprächen im Rahmen der polizeilichen strafprozessualen Telefonüberwachung auf Magnetbänder wurde inzwischen vollständig durch digitale Systeme ersetzt. Wie im 18. Tb. bereits angekündigt, ist nun flächendeckend eine einheitliche Technik eingeführt worden.

Die vom LfD im Rahmen der entwicklungsbegleitenden Stellungnahmen ausgesprochenen Empfehlungen wurden weitgehend berücksichtigt; insbesondere gilt dies für die Mechanismen der Zugriffskontrolle und der Protokollierung.

An folgenden Punkten sind datenschutzrechtliche Anforderungen noch offen:

– Die in der Vergangenheit praktizierte Unterscheidung zwischen Arbeits- und Beweisband wurde mit dem neuen digitalen System aufgegeben. Die Trennung in die Speicherung auf Festplatte bzw. MOD ist nur in zeitlicher Hinsicht von Bedeutung bzw. betrifft die unterschiedliche Speicherung von Verbindungs- und Inhaltsdaten in einem laufenden Verfahren. Nachträgliche Veränderungen an den TKÜ-Daten sind gegenwärtig nicht erkennbar. Abhilfe könnte hier durch eine nicht veränderbare, kryptografische Versiegelung der jeweiligen MOD (Hashwert) und deren Protokollierung z. B. im Rahmen der Archivierung erfolgen (vergleichbar der Medien-ID im Archivierungsprotokoll). Auf die Notwendigkeit eines Nachweises für die Authentizität und Integrität der auf MOD gespeicherten Daten wurde vom LfD bereits frühzeitig hingewiesen.

– Die Möglichkeit der Unterdrückung der Aufzeichnung von für die Ermittlungen nicht relevanten Gesprächen, insbesondere von Verteidigertelefonaten, steht derzeit immer noch nicht zur Verfügung. Aus datenschutzrechtlicher Sicht sollte zumindest die Möglichkeit der Sperrung von Gesprächen vorhanden sein.

– In Bezug auf die Auswertung von Protokolldaten sollten Such- bzw. Filtermöglichkeiten zumindest nach Benutzerkennung, Verfahren und Anschlussnummer geschaffen werden.

– Die Löschung der auf MOD gespeicherten Daten ist von der sachbearbeitenden Dienststelle zu veranlassen. In diesem Zusammenhang sollten Vorkehrungen getroffen werden, dass nicht versehentlich nach Abschluss der Verfahren entgegen § 100 b Abs. 6 StPO die gebotene Löschung unterbleibt.

– Erhebliche datenschutzrechtliche Bedenken sieht der LfD im TKÜ-Daten-Transfer zwischen den Polizeipräsidien und den nachgeordneten ermittlungsführenden Organisationseinheiten (Kriminalinspektionen) über derzeit noch unverschlüsselte Netzleitungen.

5.4 Videoaufzeichnungsgeräte in Streifenwagen der Polizei

Im Berichtszeitraum wurde die im Jahre 2000 begonnene Ausstattung der Streifenwagen der Polizei mit Videoaufzeichnungsgeräten sukzessive realisiert. Im 18. Tb. (Tz. 5.8) hat der LfD das Verfahren selbst und seine datenschutzrechtliche Bewertung dargelegt. Zwischenzeitlich ist insoweit eine Veränderung eingetreten, als die Streifenwagen die Videoausstattung im Echteinsatz nutzen.

Die vom LfD geforderte gekapselte Aufzeichnungstechnik soll in schrittweisem Austausch im Rahmen der Neubeschaffung von Dienstfahrzeugen erfolgen, so dass bis Mitte 2004 alle Streifenwagen über die „Verplombungstechnik“ verfügen werden.

Aus der Sicht des LfD ist bedeutsam, dass die unverzügliche Löschung der Aufnahmen zum Ende der Streifenfahrt gewährleistet wird, soweit diese nicht der Dokumentation zur Beweissicherung im Straf- oder Ordnungswidrigkeitenverfahren sowie eines Angriffs auf Polizeibeamte dienen.

Nachvollziehbar ist allerdings das Anliegen der Polizei, im Rahmen der Dienst- und Fachaufsicht und zur Optimierung des Einsatzverhaltens der Einsatzkräfte die Aufnahmen zum Zwecke der Einsatznachbereitung und zur Aus- und Fortbildung zu nutzen. Unter der Voraussetzung, dass Aufzeichnungen zum Zwecke der Einsatznachbereitung unmittelbar nach Auswertung der aufgezeichneten Anhalte- und Kontrollvorgänge gelöscht, die Kassettenentnahme sowie das Löschen dokumentiert und die für die Aus- und Fortbildung vorgesehenen Aufnahmen vor der Nutzung anonymisiert werden, hat der LfD zugestimmt.

Diese zentralen Forderungen fanden Aufnahme in die mit dem LfD und dem Hauptpersonalrat Polizei abgestimmte „Dienstanweisung über die Videodokumentation von Anhalte- und Kontrollvorgängen im Rahmen des Funkstreifendienstes.“

Nach derzeitigem Informationsstand des LfD kann das Löschen der Aufnahmen dann rückstandsfrei gewährleistet werden, wenn die Löschgeräte für magnetische Speichermedien in der in der Dienstanweisung zum Löschverfahren vorgeschriebenen Weise betätigt werden.

Im Übrigen wird der vom LfD im 18. Tb. vertretenen Rechtsauffassung zur Zulässigkeit der Datenerhebung mit den vorgesehenen Regelungen zur Datenerhebung durch den Einsatz technischer Mittel in der POG-Novelle Rechnung getragen.

5.5 Videoüberwachung in Gewahrsamseinrichtungen

Zur Frage, ob und unter welchen Modalitäten eine optische Überwachung von Gewahrsamszellen bei der Polizei mit Hilfe von Videokameras zulässig ist, legte das Ministerium des Innern und für Sport am 19. Dezember 2001 den Entwurf der Gewahrsamsordnung für die Polizei des Landes Rheinland-Pfalz vor. Diese Regelung erlaubt den offenen Einsatz technischer Mittel zur Bildübertragung (Videoüberwachung) in Vorräumen von Gewahrsamseinrichtungen dann, wenn es zum Schutz von Polizeibeamten oder Dritten erforderlich erscheint. Gewahrsamsräume hingegen sollen durch den offenen Einsatz technischer Mittel zur Abwehr gegenwärtiger Gefahren für Leib und Leben der in Gewahrsam befindlichen Personen beobachtet werden können. Nach den vorgesehenen Bestimmungen wird das Speichern der dabei erhobenen personenbezogenen Daten als unzulässig angesehen. Darüber hinaus ist die Beobachtung dem Betroffenen bekannt zu geben und die Datenerhebung durch ein optisches Signal anzuzeigen.

Zwar entsprechen die einschränkenden Voraussetzungen grundsätzlich dem datenschutzrechtlichen Anliegen des Persönlichkeitsschutzes, Sorge begründet die Überwachung jedoch, weil durch sie ein Einstieg in die Videoüberwachung bei Menschen in geschlossenen Bereichen geschaffen werden könnte. Die im Rahmen einer Länderumfrage gewonnenen Erkenntnisse zeigen, dass bisher kein Bundesland den Einsatz von Videotechnik in Gewahrsamsräumen durch landesweite Verwaltungsvorschriften regelt. Gleichwohl wird die Videotechnik in einigen Polizeidienststellen eingesetzt und in behördlichen Gewahrsamsanordnungen geregelt. Es besteht allgemeine Übereinstimmung, dass in engen Grenzen (zur Verhinderung von Todesfällen) die Videoüberwachung dann hinnehmbar sei, wenn keine andere Möglichkeit bestehe. Die vom LfD angeregte Prüfung von Protokollierungsmöglichkeiten der Videoüberwachung hinsichtlich der Anordnung, Zeitpunkt und Dauer der Maßnahmen wurde in die am 8. März 2003 in Kraft gesetzte Gewahrsamsordnung für die Polizei (veröffentlicht im MinBl. 55/2003 Nr. 7, S. 292 ff.) aufgenommen.

Derzeit sind in zwei präsidialen Zentralgewahrsamseinrichtungen technische Mittel zur Überwachung von insgesamt sechs Gewahrsamszellen vorgesehen. Die Beobachtung der Flure vor den Gewahrsamszellen ist in drei Gewahrsamseinrichtungen möglich.

5.6 Auskunftserteilungen durch die Polizei an die Betroffenen

Für die Bürger kann es höchst bedeutsam sein, dass die Polizei Informationen über sie gespeichert hat. In vielen Zusammenhängen werden Polizeidienststellen danach gefragt, ob sie Erkenntnisse über eine Person haben. Beispiele:

– Einstellung als Mitarbeiter eines auf einem Flugplatz tätigen Unternehmens
– Einstellung als Anwärter für den Polizeidienst
– Regelanfrage vor einer Einbürgerung etc.

Deshalb ist es für den Betroffenen wichtig zu wissen, was die Polizei gespeichert hat, und was sie weitergibt. Auch unabhängig von den genannten Beispielsfällen ist es nicht unwichtig zu wissen, welche Hintergrundinformationen der Polizeibeamte besitzt, dem man – etwa bei einer Anzeigenerstattung oder bei einer Zeugenvernehmung – gegenübersitzt.

Das Auskunftsrecht des Betroffenen gegenüber der Polizei ergibt sich aus § 25 f POG. Danach gilt: Die allgemeinen Ordnungsbehörden und die Polizei haben dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Informationen zu erteilen. Ein Anspruch auf Auskunft besteht insoweit nicht, als dadurch die Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben erschwert oder gefährdet würde, sie dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder ihr berechtigte Interessen einer dritten Person entgegenstehen.

In der Praxis wurde und wird dieses Recht nur von wenigen in Anspruch genommen. Nach den beim LKA und den Polizeipräsidien eingeholten Schätzungen dürften es nicht mehr als ca. 120 Fälle pro Jahr sein. Nicht selten haben diese Anträge aber einen für die Existenz der Fragesteller wichtigen Hintergrund. Natürlich ist es auch bedeutsam, wann diese Speicherungen gelöscht werden (s. dazu unten Tz. 5.14). Die Betroffenen können ihr Recht auf Löschung, Berichtigung und Sperrung (§ 6 Abs. 1 LDSG) nur dann wirksam ausüben, wenn sie über den Inhalt von Datenspeicherungen umfassend informiert sind.

Der Landesbeauftragte für den Datenschutz musste feststellen, dass die Auskunftserteilung durch die Polizei nicht immer vorbildlich war: Nicht selten wurde nur eine Auskunft über die Speicherung (oder auch das Fehlen einer Speicherung) in den zentralen polizeilichen Informationssystemen INPOL/POLIS erteilt. Für die Betroffenen kann aber gerade entscheidend sein, was in den örtlichen Dateien der Polizei, insbesondere in der polizeilichen Vorgangsverwaltung (im System „POLADIS“), gespeichert ist. Zwar kann nur die speichernde Dienststelle selbst darauf Zugriff nehmen. Anfragende Dienststellen anderer Behörden aber erhalten daraus nicht selten Auskunft. Dort werden beispielsweise auch Anzeigen verärgerter Nachbarn über Ruhestörungen, vermeintliche Beleidigungen oder auch vermeintliche Sachbeschädigungen durch das Beschneiden einer Grenzhecke gespeichert. Die Speicherfristen sind zudem zum Teil sehr lang (Vorgangsverwaltungsdaten über den Verdachtsfall einer Nötigung im Straßenverkehr werden beispielsweise regelmäßig noch zehn Jahre nach Abschluss der Sachbearbeitung gespeichert).

Außerdem wandern solche Daten auch in die polizeiliche Kriminalstatistik. Dort dürfen sie zwar nur höchst ausnahmsweise reidentifiziert und gegenüber Einzelpersonen genutzt werden; dennoch handelt es sich hier um personenbeziehbare Speicherungen.

Vor diesem Hintergrund hat der LfD darauf gedrungen, grundsätzlich (wenn kein Grund zur Auskunftsverweigerung im Sinne des Gesetzes vorliegt) umfassend Auskunft zu erteilen unter Einschluss der Speicherungen im polizeilichen Vorgangsbearbeitungssystem POLADIS und der Speicherungen in der polizeilichen Kriminalstatistik, um den Betroffenen ein zutreffendes Bild zu vermitteln. Das Ministerium des Innern und für Sport stand diesem Anliegen aufgeschlossen gegenüber.

Künftig werden die Auskünfte der Polizei etwa folgenden Inhalt haben:

„Im polizeilichen Informationssystem „INPOL“, das allen Polizeidienststellen bundesweit zum Abruf zur Verfügung steht, sind keine/folgende Informationen über Sie gespeichert:
Die Frist, nach deren Ablauf eine Prüfung über die weitere Speicherung dieser Daten erfolgt („Prüffrist“) ist auf den ..... festgelegt worden.

Im polizeilichen Informationssystem „POLIS“, das nur den rheinland-pfälzischen Polizeidienststellen zum Abruf zur Verfügung steht, sind keine/folgende Informationen über Sie gespeichert:
Die Frist, nach deren Ablauf eine Prüfung über die weitere Speicherung dieser Daten erfolgt („Prüffrist“) ist auf den ..... festgelegt worden.

Im polizeilichen Vorgangsbearbeitungssystem „POLADIS“, das ausschließlich die örtlich zuständige Polizeidienststelle im Abrufverfahren nutzen kann, waren bei der für Ihren Wohnsitz zuständigen Polizeidienststelle keine/folgende Informationen über Sie gespeichert:
Die Frist, nach deren Ablauf eine Prüfung über die weitere Speicherung dieser Daten erfolgt („Prüffrist“) ist auf den ..... festgelegt worden.

Darüber hinaus enthält die polizeiliche Kriminalstatistik dann anonymisierte Angaben über die Sie betreffenden Vorgänge, wenn Sie als Verdächtigter in polizeiliche Ermittlungen einbezogen worden sind. Diese Angaben dürfen aber grundsätzlich nicht mehr auf Ihre Person zurückbezogen werden, so dass sie grundsätzlich keine Auswirkungen Ihnen gegenüber mehr haben können.“

5.7 Anspruch von Eltern gegen die Polizei auf Auskunftserteilung über Kinder

Ein Erziehungsberechtigter wollte für seinen minderjährigen Sohn das Auskunftsrecht über zur Person des Sohnes gespeicherte Daten wahrnehmen. Er fragte an, ob die Auffassung des LKA, Voraussetzung einer Auskunftserteilung sei die Vorlage einer Kopie des Personalausweises des Sohnes sowie einer von diesem ausgestellten Vollmachtserklärung, zutreffend ist.

Der Auskunftsanspruch soll den Einzelnen in die Lage versetzen, sich darüber Klarheit zu verschaffen, welche ihn betreffenden Informationen bei öffentlichen Stellen bekannt sind. In Rheinland-Pfalz ist dieser Anspruch in der Landesverfassung (Art. 4 a) verankert und in verschiedenen so genannten bereichsspezifischen Gesetzen konkretisiert. Der Anspruch des Bürgers auf Auskunftserteilung gegenüber der Polizei ist in § 25 f POG im Einzelnen geregelt. Voraussetzung für die Auskunftserteilung ist ein Antrag des Betroffenen. Ein besonderes Formerfordernis für den Antrag ist nicht vorgesehen. Er kann schriftlich, im Rahmen der Vorsprache bei der Behörde oder auch telefonisch gestellt werden. Im Falle eines mündlichen Antrags oder bei einer E-Mail-Anfrage hat sich die öffentliche Stelle allerdings zu vergewissern, ob der Antragsteller mit der Person, über die Auskunft begehrt wird, identisch ist. Das kann z. B. durch die Vorlage eines entsprechenden Ausweisdokumentes erfolgen.

Dem Betroffenen ist Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Die Stellung des Antrags auf Auskunft setzt nicht zwingend voraus, dass der Betroffene geschäftsfähig ist. Vielmehr reicht es aus, dass der Betroffene in der Lage ist, die Bedeutung des Auskunftsverlangens beurteilen zu können. Dies folgt daraus, dass der Auskunftsanspruch eine Auswirkung des allgemeinen Persönlichkeitsrechts in Gestalt des Grundrechts auf Datenschutz darstellt. Maßgeblich ist also für die Geltendmachung die Grundrechtsmündigkeit des Betroffenen selbst. Dabei kommt es nicht allein auf das Alter an, sondern auf den individuellen Reifegrad des Betroffenen sowie auf den Sachzusammenhang, in dem der Auskunftsanspruch steht. Die Fähigkeit, die Tragweite der Entscheidung abzuschätzen, kann umso eher angenommen werden, je näher der Minderjährige der Volljährigkeitsgrenze ist und dürfte ab einem Alter von 14 bis 15 Jahren im Bereich des Datenschutzgrundrechts vorliegen. Fehlt diese Einsichtsfähigkeit, bedarf es der Antragstellung durch den gesetzlichen Vertreter des Betroffenen.

Ansonsten aber kann der gesetzliche Vertreter nur unter den Bedingungen, unter denen generell ein Vertreter für den Vertretenen handeln kann, diesen Anspruch geltend machen. Aus der Elternstellung ergibt sich bei grundrechtsmündigen Kindern grundsätzlich kein eigener datenschutzrechtlich begründeter Auskunftsanspruch gegenüber den speichernden Stellen.

Ob der Erziehungsberechtigte unabhängig von diesem datenschutzrechtlichen Auskunftsanspruch einen Informationsanspruch gegenüber der Polizei hat, um im Rahmen seines Erziehungsrechts auf den Minderjährigen einwirken zu können, ist von der Polizei im Rahmen ihres pflichtgemäßen Ermessens gem. § 25 a POG zu entscheiden. Die Unterrichtung des Erziehungsberechtigten über polizeiliche Erkenntnisse bezüglich des Kindes ist generell sicher geeignet, die polizeilichen Aufgaben der Gefahrenabwehr und der Strafverfolgung zu fördern. Dies hängt aber vom jeweiligen Einzelfall ab und ist von der Polizei selbst zu beurteilen.

Von der speichernden Stelle kann bestimmt werden, welche Anforderungen an die Identifizierung des auskunftsersuchenden Betroffenen und an den Nachweis der Vertretungsmacht zu stellen sind. Da es sich um die Geltendmachung eines grundsätzlich höchstpersönlichen Rechts handelt, werden die Anforderungen streng sein müssen. Das kann durchaus dazu führen, dass im Fall der Vertretung des Minderjährigen durch seinen Erziehungsberechtigten ein schriftlicher Antrag und die Einverständniserklärung des betroffenen Minderjährigen für erforderlich angesehen werden.

Vor dem Hintergrund dieser Rechtslage könnten dann Zweifel an der Ausübung des pflichtgemäßen Ermessens des LKA bestehen, wenn das Kind in einem Alter wäre, das deutlich unter 15 Jahren läge. Gegen die Forderung einer Kopie des Personalausweises zur Feststellung der Identität von Antragsteller und Auskunftsberechtigten bestehen keine datenschutzrechtlichen Bedenken. Das LKA hatte sich damit im Rahmen der verfassungsrechtlichen und gesetzlichen Vorgaben gehalten.

5.8 Maßnahmen der „Polizeilichen Beobachtung“ zu vorbeugenden Zwecken

Im System INPOL werden unter der Verfahrensbezeichnung „Remo“, „Limo“ und „Aumo“ Personen erfasst, die verdächtig sind, rechtsextremistisch, linksextremistisch oder ausländerextremistisch motivierte Straftaten zu begehen. Bei einigen Personen war zusätzlich vermerkt, dass ihr Antreffen bei polizeilichen Kontrollen oder sonstigen polizeilichen Maßnahmen an die ausschreibende Dienststelle gemeldet werden sollte.

Hierbei handelte es sich nach Auffassung des LfD um Maßnahmen der polizeilichen Beobachtung, die nur auf der Basis der entsprechenden Rechtsgrundlagen in der StPO (§ 163 e) oder der jeweiligen Polizeigesetze zulässig sind. In erster Linie ist dafür eine richterliche Anordnung erforderlich.

Das Ministerium des Innern und für Sport hat sich dieser Auffassung grundsätzlich angeschlossen und veranlasst, dass bei den Eintragungen in diese Dateien keine Rückmeldungen an die ausschreibende Polizeibehörde mehr verlangt werden. Die zur polizeilichen Beobachtung vorgesehene Neuregelung im vorliegenden POG-Entwurf (s. o. Tz. 5.1) ist aus der Sicht des LfD wegen des fehlenden Richtervorbehalts für diese eingreifende Maßnahme verbesserungsbedürftig.

5.9 Speicherungen in polizeilichen Dateien „ohne Delikt“

Eine gezielte Überprüfung der Speicherungen in den Kriminalakten lenkte die Aufmerksamkeit auf folgenden Fall, der ohne Angabe eines Delikts, also „ODEL“, im polizeilichen Informationssystem POLIS gespeichert war:

Der Betroffene ist Vermieter von Ferienappartements in den USA. Er wurde nachts häufig durch Werbefaxe aus den USA gestört, die sein Gerät blockierten und ihn auch sonst ärgerten. Er rief deshalb – im Oktober 2001, einen Monat nach dem Anschlag auf das WTC – bei der US-Botschaft an und beschwerte sich; dabei machte er wohl einen erregten Eindruck; jedenfalls äußerte er sinngemäß, wenn die Botschaft nicht für Abhilfe sorge, werde er sich entsprechend wehren.

Dieser Vorgang führte zu einem Besuch der Polizei, die den Kaufmann „sensibilisierte“, wie es im polizeilichen Bericht heißt; außerdem wurde er mit einer Prüffrist von fünf Jahren in POLIS eingestellt. Ein Delikt konnte naturgemäß nicht eingegeben werden, da keines begangen worden war. Die Polizei hielt den Mann zunächst aber für gefährlich genug, um ihn zu speichern.

Aufgrund der Einwände des LfD wurde die Löschung veranlasst.

5.10 Nutzung von Lichtbildern aus dem Pass- und Personalausweisregister für Bußgeldverfahren

Von einer Verbandsgemeindeverwaltung wurde der LfD um Beurteilung der Zulässigkeit des Abgleichs von Passbildern anderer Personen im Rahmen der Fahrerermittlung zur Verfolgung von Straßenverkehrsordnungswidrigkeiten ersucht. Er vertritt folgende Rechtsauffassung, die ihren Niederschlag im Rundschreiben des Ministeriums des Innern und für Sport vom 26. März 2002 (MinBl. S. 308) gefunden hat.

In allen Fällen, in denen nicht von vornherein klar ist, ob Fahrzeughalter und Fahrer identisch sind, ist zunächst dem Fahrzeughalter im Rahmen des Anhörungsverfahrens Gelegenheit zu geben, die auf dem Radarfoto abgebildete Person zu identifizieren. 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 dann abgeglichen werden, wenn die Ermittlung des Fahrzeugfahrers ansonsten unmöglich oder der Aufwand unverhältnismäßig hoch wäre, unabhängig von der Höhe der in Rede stehenden Bußgeldandrohung.

Angemessen erscheint, im Rahmen der Anhörung – falls eine solche erfolgt – den Betroffenen darauf hinzuweisen, dass das Radarfoto mit im Pass- oder Personalausweisregister hinterlegten Fotos verglichen werden kann, wenn er sich nicht zur Sache äußern will.

Führt auch dieser Abgleich nicht zur Ermittlung des Fahrers, hält der LfD es im Rahmen der Verhältnismäßigkeit für erforderlich, zunächst den als Fahrer in Betracht kommenden Familienangehörigen die Gelegenheit der Anhörung einzuräumen. Tragen die Familienangehörigen des Halters nicht zur Fahrerermittlung bei, ist der Abgleich mit im Pass- oder Personalausweisregister hinterlegten Fotos der Familienangehörigen zulässig und verhältnismäßig, denn im Vergleich zur Nachbarschaftsbefragung stellt er den weniger belastenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar.

Ein zulässiges und angebrachtes Aufklärungsmittel zur Fahrerermittlung ist auch die Befragung von Familienangehörigen, Nachbarn und sonstigen Dritten. Wegen des verhältnismäßig intensiven Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen kann die Befragung Dritter aber aus datenschutzrechtlicher Sicht nur dann angezeigt sein, wenn weniger einschneidende Maßnahmen erfolglos geblieben oder unmöglich sind.

5.11 Örtliche Feststellungen

Neben zahlreichen Beratungs- bzw. Informationsgesprächen bei der Projektgruppe des Innenministeriums und beim Landeskriminalamt zur Entwicklung der EDV-Nachfolgesysteme POLADIS.net und POLIS.net im Hinblick auf die Einführung von RIVAR (Rheinland-Pfälzisches Informations-, Vorgangsbearbeitungs- Auswerte- und Recherchesystem) fanden im Berichtszeitraum in den fünf Präsidialbereichen bei 23 Polizeidienststellen, bei einer Verfassungsschutz- und einer Ausländerbehörde örtliche Feststellungen statt. Beanstandungen wurden hierbei nicht ausgesprochen.

5.11.1 Polizeiliches Vorgangsbearbeitungssystem POLADIS

Bei diesen örtlichen Feststellungen war ein regelmäßiger Schwerpunkt die polizeiliche Vorgangsdatenspeicherung, die parallel in verschiedenen Systemen des polizeilichen anwenderorientierten dezentralen Informationssystems POLADIS erfolgt: POLADIS 95 für die Jahre 1996 bis 1999, POLADIS-neu für die Jahre ab 2000. Nunmehr ist POLADIS.net im Einsatz. Die Datenhaltung in verschiedenen Systemen bringt Schwierigkeiten mit sich: Für gleichartige Daten gelten unterschiedliche technische und organisatorische Bedingungen und Regelungen.

Technisch nicht realisiert war in POLADIS 95 das Heraustrennen von Daten aus dem Datenvollbestand. Damit steht die im Fachkonzept „Archivierung von Vorgangslöschungen im POLADIS-95-Verfahren“ vorgesehene Archivierung der für die Behördendokumentation erforderlichen Daten (Vorgangsverwaltungsdaten) den Anwendern dieser ersten Version von POLADIS 95 nicht zur Verfügung. Diese Option eröffnet allen zugriffsberechtigten Mitarbeitern die Recherche im Datenvollbestand, begründet also auch die Verfügbarkeit der Daten, die für die Aufgabenerfüllung nicht mehr erforderlich sind. Die Intervention des LfD führte insoweit zu einem in weiten Teilen zufrieden stellenden Kompromiss, als im Rahmen einer Interimslösung die Zugriffsberechtigungen auf ein Mindestmaß beschränkt, Archivierungsmodalitäten (spätestens drei Jahre nach Abschluss der Sachbearbeitung) entwickelt und wegen der je nach Organisationseinheit gegebenen Unterschiede in Verwendungszweck, Inhalt und Schutzbedarf der Datenbestände dienststellenspezifische Löschfristen (maximal zehn Jahre nach Ermittlungsabschluss) festgelegt worden sind. Löschmodalitäten, die eine Trennung zwischen den Daten, die für die aktuelle Bearbeitung der Ermittlungsvorgänge benötigt werden (Vorgangssachbearbeitungsdaten) und den Registraturdaten (Vorgangsverwaltungsdaten) vorsehen, sind erst mit der Einführung der zweiten Version von POLADIS (POLADIS-neu) zur Anwendung gekommen.

5.11.2 Rückmeldungen an die Polizei über das Ergebnis von Strafverfahren

In der Vergangenheit hatte der LfD wiederholt festgestellt, dass in einigen Kriminalakten (Kriminalpolizeilichen Sammlungen – KpS) die Informationen über die Ergebnisse von Strafverfahren durch die Staatsanwaltschaft an die sachbearbeitende Polizeidienststelle („MiStra-Rückläufe“) fehlten. Der von ihm angeregten Verfahrensweise, bei Fehlen der MiStra-Rückläufe eine Nachfragepflicht der Polizeidienststellen vorzusehen, wurde im Berichtszeitraum insoweit Rechnung getragen, als eine große Anzahl überprüfter Kriminalakten MiStra-Rückläufe enthielten. Eine Polizeidienststelle hatte sogar die telefonische Anforderung des MiStra-Rücklaufs schriftlich dokumentiert.

Trotz dieser positiven Bilanz im MiStra-Rücklauf-Verfahren bestand dennoch bei örtlichen Feststellungen Anlass, Verbesserungsvorschläge aus datenschutzrechtlicher Sicht zu formulieren, wobei in allen Fällen Einvernehmen mit dem Ministerium des Innern und für Sport erzielt wurde.

5.11.3 Einzelfragen

Im Einzelnen sah der LfD bei folgenden Themen Handlungsbedarf:

– Zur Erfüllung polizeilicher Aufgaben auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr führt die Polizei Kriminalakten (KpS). Ist der Polizei eine Person als Gefährder oder Tatverdächtiger bekannt geworden, werden die personenbezogenen Informationen zu dieser Person grundsätzlich sowohl im Polizeilichen Informationssystem (POLIS) als auch in der KpS erfasst. Dabei können beispielsweise Informationen über frühere, nicht mehr im Einwohnermelderegister geführte Aufenthaltsorte von Personen für die polizeiliche Tätigkeit bedeutsam sein. Solche Hinweise werden in POLIS als Zusatzinformation (Z-Gruppe) gespeichert. Löscht die datenerfassende Stelle die zu dieser Information vorgehaltene KpS der betroffenen Person, hält aber die Zusatzinformationen zum früheren Aufenthalt weiterhin zur polizeilichen Aufgabenerfüllung für erforderlich, begegnet diese Verfahrensweise datenschutzrechtlichen Bedenken, weil der Aktenrückhalt fehlt und nicht mehr nachvollzogen werden kann, wer die Information ursprünglich gespeichert hatte. Die Erörterung dieser Problematik mit dem Ministerium des Innern und für Sport führte dazu, dass die Polizeidienststellen angewiesen wurden, bei Z-Gruppen-Einträgen die Eingabestelle (Terminalkennung) und den Erfassungszeitpunkt zu dokumentieren.

Neben den Zusatzinformationen enthält POLIS im Datenfeld „Sondervermerk (USV)“ auch Angaben zu Delikten, die Tatverdächtigen zur Last gelegt werden. Bei einigen Polizeidienststellen war eine Diskrepanz zwischen den Einträgen in den Kriminalakten der jeweils Beschuldigten und den im entsprechenden Datenfeld eingetragenen Tatvorwürfen aufgefallen. Diese unterschiedlichen Deliktsbezeichnungen sind darauf zurückzuführen, dass eingehende MiStra vor der Aufnahme in die jeweilige Kriminalakte nicht mit dem Eintrag im Datenfeld „Sondervermerk“ insoweit abgeglichen worden waren, ob die bei Anzeigenerstattung von der Polizei vorgenommene Deliktsbezeichnung von der Justiz bestätigt oder sich eine abweichende rechtliche Einordnung des Tatvorwurfs ergeben hatte. Auf Grund der Empfehlung des LfD wurden die Polizeibehörden und -einrichtungen vom Ministerium des Innern und für Sport zum Abgleich der MiStra-Rückläufe zwischen vorgelegtem Delikt und der Entscheidung der Justiz verpflichtet.

– Bei einzelnen Dienststellen waren Prüf- und Aussonderungsfristen der Kriminalakten (KpS) bei Delikten mit Bagatellcharakter unangemessen lang gewählt worden. Die Daten mussten gelöscht werden.

– Im Rahmen der Kriminalakten-Prüfung fiel auf, dass eine große Anzahl der Formblätter, die eine Kurzinformation zum Ermittlungsverfahren, Hinweise zu Tatverdächtigen und kriminaltaktische Besonderheiten enthalten (Merkblätter), nur unzureichend die Gesamtumstände der Tatbegehung schilderten und damit für eine eventuell zu stellende Rückfallprognose und die Festlegung der Aufbewahrungsdauer ungeeignet erschienen. Auf Empfehlung des LfD hin wurden die nichtssagenden Merkblätter gelöscht und die Ergebnisse der Überprüfung vom Ministerium des Innern und für Sport zum Anlass genommen, die Kontrolle der Kriminalakten-Führung zu intensivieren.

– Wie bereits in den vorhergehenden Tätigkeitsberichten geschildert, waren auch in diesem Berichtszeitraum nicht bei allen Dienststellen entweder die erforderlichen Aufzeichnungen über Einsichtnahmen in die Lichtbildkartei des Pass- und Ausweisregisters zur Verfolgung von Verkehrsordnungswidrigkeiten oder die schriftliche Dokumentation der für die Einsichtnahme Ermächtigten vorhanden.

– Auch die Pflicht zur Zusatzprotokollierung bei POLIS-Abfragen für andere musste bei einigen Dienststellen – wie bereits in der Vergangenheit häufig festgestellt – erneut in Erinnerung gebracht werden.

– Die im Zusammenhang mit der Datei „Castor“ (s. unten Tz. 5.13) aufgefallenen Unzulänglichkeiten hinsichtlich der Eingabe- und Verarbeitungskontrolle – es war im Nachhinein nicht mehr nachvollziehbar, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden waren sowie wer wann welche Daten gespeichert hatte – wurden auf Empfehlung des LfD behoben. Die Frage der Nachvollziehbarkeit von Datenspeicherungen und -zugriffen hat durch diesen Vorgang nunmehr insgesamt bei den polizeilichen Datenspeicherungen erhöhte Aufmerksamkeit erfahren; es ist zu erwarten, dass damit künftig vergleichbare Probleme nicht mehr auftreten.

5.12 Anmeldung von EDV-Verfahren nach § 27 Abs. 1 LDSG

Insbesondere im Jahr 2002 erreichten die Anmeldungen von Verbunddateien beim BKA und die als landesweite oder Einzel-Dateien der Polizeibehörden errichteten Dateien zahlenmäßig einen Höhepunkt. Mit Blick auf die Vorgaben der Europäischen Datenschutzrichtlinie, die auch im LDSG (s. Tz. 2.1) ihren Niederschlag fanden, gab der LfD hierzu zahlreiche Anregungen hinsichtlich technisch-organisatorischer Maßnahmen zum Schutz personenbezogener Daten, insbesondere zur Nachvollziehbarkeit von ändernden und lesenden Datenzugriffen (vgl. auch Tz. 5.11 und 5.13). Darüber hinaus bezogen sich die Empfehlungen auf Aspekte der Konkretisierung des betroffenen Personenkreises, der Prüf- und Löschfristen personenbezogener Daten sowie der Einleitung der Mitbestimmungsverfahren bei Dateien, die geeignet sind, Verhaltens- und Leistungsprofile der Betroffenen zu erstellen.

So sind beispielsweise in der Eingabemaske zur Person in der Datei „Überörtliche Eigentumskriminalität (ÜEK)“ diverse Rollen für am Ermittlungsverfahren beteiligte Personen hinterlegt. Durch das Einblenden einer definierten Vorauswahl in diesem Drop-Down-Menü kann der zu erfassenden Person eine bestimmte „Rolle“ zugewiesen werden. Da aber sowohl bei der Zentralstelle LKA als auch bei einer Flächendienststelle nur drei verschiedene Rollen genutzt wurden, war mit dem Ministerium des Innern und für Sport zu erörtern, ob die Abbildung aller denkbaren Erfassungsmöglichkeiten erforderlich ist.

5.13 Datenerhebung und -verarbeitung in der Castor-Datei

Zur Abwehr im Einzelfall bestehender Gefahrenlagen in Zusammenhang mit Castor-Transporten war die Datei „Castor“ vom 1. August 2001 bis 3. Dezember 2002 als lokal beschränkte automatisierte Datenverarbeitung von einem Polzeipräsidium betrieben worden. Speicherungen erfolgten zu den Personen, gegen die auf Grund einer Straftat oder Ordnungswidrigkeit im Zusammenhang mit Castor-Transporten Ermittlungen geführt wurden oder Adressaten polizeilicher Maßnahmen zur Gefahrenabwehr geworden waren. Während der Nutzung der Datei begehrten Privatpersonen verschiedentlich Auskünfte über zu ihrer Person in dieser Datei gespeicherte Daten. Im Einzelnen lagen dem LfD folgende Anträge vor:

– Ein Petent rügte beim LfD das Verhalten eines behördlichen Datenschutzbeauftragten (bDSB), der ihm telefonisch Auskunft über in der Datei Castor zu seiner Person gespeicherte Daten erteilt habe. Er war der Meinung, seine Identität sei nicht ausreichend überprüft worden. Obwohl die für die Datenverarbeitung verantwortliche Stelle (sie bestimmt gemäß § 18 Abs. 3 Satz 3 LDSG nach pflichtgemäßem Ermessen die Form der Auskunftserteilung) zur Auffassung gelangt war, die Identität sei hinreichend festgestellt, nahm die betroffene Polizeibehörde die Eingabe dennoch zum Anlass, die generelle Anweisung zu erteilen, künftig von telefonischen Auskunftserteilungen Abstand zu nehmen.

– Auf Anregung des LfD führte die von einem Petenten vorgetragene Schilderung, ein bDSB habe ihm eine dritte Person betreffende Daten übermittelt, zu einer Rüge des Fehlverhaltens des bDSB durch die Behördenleitung.

– In zwei Fällen hatten Petenten den LfD um Überprüfung der Rechtmäßigkeit der Castor-Datei, der Zulässigkeit von Datenspeicherungen und um Prüfung der Vollständigkeit behördlicher Auskünfte gebeten. Sowohl die Errichtungsanordnung als auch die beabsichtigte Nutzung der Datei boten zunächst keinen Anlass für datenschutzrechtliche Bedenken. Bei einer Prüfung der Datei im Wirkbetrieb fielen jedoch folgende Mängel auf, deren unverzügliche Beseitigung auf Empfehlung des LfD vorgenommen wurde:

– Anhand der in der Datei Castor gespeicherten Informationen konnten getroffene polizeiliche Maßnahmen nachträglich nicht mehr präzise nachvollzogen werden. So blieb unklar, ob Betroffene auf der Grundlage des § 10 Abs. 2 Satz 3 (Festhalten zur Identitätsfeststellung) oder gemäß § 14 Abs. 1 Nr. 2 POG (zur Verhinderung der Begehung oder Fortsetzung einer Straftat oder Ordnungswidrigkeit) festgehalten worden waren. Offen blieb ebenfalls, ob das Strafprozessrecht (wegen öffentlichen Aufrufs zu Straftaten) oder § 14 Abs. 1 Nr. 2 POG Rechtsgrundlage der getroffenen Maßnahmen war, als ein Betroffener für die Einsatzdauer festgehalten wurde. Die sorgfältige und korrekte Formulierung von Tatbestandsmerkmalen der zur Last gelegten Straftaten oder Ordnungswidrigkeiten ist aber aus datenschutzrechtlicher Sicht ein wesentliches Element von Datenspeicherungen, die eindeutig und zutreffend sein müssen.

– Auch dem von einem Petenten vorgetragenen Vorwurf, er sei nicht umfassend über den ihn betreffenden, zwischenzeitlich gelöschten Datenbestand schriftlich unterrichtet worden, konnte von der Behördenleitung durch die Intervention des LfD abgeholfen werden.

Mit der zwischenzeitlich eingetretenen Lageberuhigung bei Castor-Transporten war die automatisierte Verarbeitung der Störerdaten nicht mehr erforderlich, so dass der Betrieb der Datei am 3. Dezember 2002 eingestellt werden konnte.

5.14 Eignungsüberprüfung für den Polizeidienst mit polizeilichen Daten?

Weil der Petent einen ablehnenden Bescheid auf seine Bewerbung zur Einstellung in den Polizeidienst eines anderen Bundeslandes erhalten hatte, ersuchte er den LfD einerseits um Überprüfung der Zulässigkeit der Datenübermittlung durch rheinland-pfälzische Polizeidienststellen an die betreffende Polizeischule und andererseits um Weiterleitung seines Löschungsantrags an die datenspeichernde Stelle. Im Zusammenhang mit der Einstellung von Personen in den Polizeidienst ist eine Datenübermittlung dann zulässig, wenn eine Einstellungsentscheidung ohne Kenntnis der zu übermittelnden Daten eine polizeiliche Gefahr begründen würde und wenn der betroffene Bewerber vorher in die Datennutzung eingewilligt hat. Allerdings dürfen nur solche Daten übermittelt werden, die zum Zeitpunkt der Auskunft noch rechtmäßig im jeweiligen polizeilichen Datenverarbeitungssystem gespeichert sind. Vor diesem Hintergrund hat der LfD keine grundsätzlichen Bedenken gegen die im vorliegenden Fall erfolgten Datenübermittlungen geäußert; Zweifel äußerte er nur hinsichtlich der Speicherdauer und damit der Übermittlung von Daten zu einem Ermittlungsverfahren aus dem Jahre 1998. Auf seine Empfehlung hin wurden die Daten zu diesem Ermittlungsverfahren gelöscht. Da aber die anderen erfolgten Datenspeicherungen und -übermittlungen zulässig waren, änderte sich an dem für den Beschwerdeführer negativen Ergebnis des Einstellungsverfahrens nichts.

5.15 Folgenschwere Verwechslung im Zusammenhang mit einer Zuverlässigkeitsüberprüfung

Ein Gebäudereinigungsunternehmer hatte den LfD um Auskunft über zu seiner Person gespeicherte Daten ersucht, da ihm der bestehende Reinigungsvertrag mit einem Geldinstitut fristlos gekündigt und die Fortführung der Reinigungsarbeiten wegen einer Speicherung seiner personenbezogenen Daten in INPOL untersagt worden war. Die Recherchen des LfD ergaben, dass die Identität eines in einem Ermittlungsverfahren wegen räuberischer Erpressung benannten Tatverdächtigen falsch festgestellt und in INPOL bundesweit gespeichert worden war. Offenbar existierten zwei Personen gleichen Familien- und Vornamens, jedoch mit unterschiedlichen Geburtsdaten und -orten. Der Polizeibeamte hatte versäumt, durch sachgerechte Ermittlungen den richtigen Verdächtigen zu verifizieren. Stattdessen hatte er die in INPOL vorgefundenen Personendaten ungeprüft und fälschlicherweise dem Gebäudereinigungsunternehmer zugeordnet. Dem datenschutzrechtlichen Anliegen, sowohl die bestehende kriminalpolizeiliche Akte und den INPOL-Datensatz zu löschen als auch die Korrektur der staatsanwaltschaftlichen Verfahrensregister zu veranlassen, wurde neben der Richtigstellung beim Auftraggeber des Petenten unverzüglich Rechnung getragen.

5.16 Lichtbilder auf der Müllkippe

Auf einer Müllumschlagstation hatte ein Bürger in Müllsäcken „ein Bündel Polizeifotos“ gefunden und mitgenommen. Weil der Finder einige der auf den Bildern abgelichteten Personen erkannte, übergab er die Aufnahmen an die Abgebildeten und informierte die örtliche Presse. Der Polizei gelang es, alle gefundenen Lichtbilder sicherzustellen. Wie sich später herausstellte, handelte es sich bei dem Fund um überwiegend in den 80er Jahren von einer Polizeibehörde aufgenommene erkennungsdienstliche Lichtbilder Tatverdächtiger.

Nach der für die betroffene Polizeibehörde geltenden „Dienstvereinbarung über die Sammlung und Entsorgung anfallender Abfälle“ aus dem Jahr 1995 sind Akten mit schutzwürdigen personenbezogenen Daten getrennt von sonstigem Papiermüll zu sammeln und zu vernichten. Wie die Lichtbilder trotz der bestehenden Regelungen in den Müll gelangen konnten, erklärte die Polizei damit, dass ein Polizeibeamter ungeachtet der bestehenden Anweisung Lichtbilder, die vernichtet werden sollten, in seinem Büro aufbewahrt und später irrtümlich in ein Behältnis für allgemeinen Papiermüll gelegt hatte. Dieser Papiermüll war deshalb nicht durch den vertraglich verpflichteten Entsorgungsunternehmer im Beisein von Polizeibediensteten vernichtet, sondern zu der betreffenden Müllumschlagstation transportiert worden.

Bei anschließend vom LfD durchgeführten örtlichen Feststellungen fanden Überprüfungen der Entnahme- und Dokumentationsmodalitäten von Lichtbildern und Kriminalakten (kriminalpolizeiliche Sammlungen – KpS –) statt mit dem Ergebnis, dass die Nachvollziehbarkeit derAusleihe von KpS und Lichtbbildern in unterschiedlichster Art und Weise geregelt war. Während einige Polizeidienststellen Lichtbilder nur in den KpS und in einer Präsenzkartei vorhalten, besteht bei manchen Fachkommissariaten auch die Möglichkeit, in aktuellen Einzelfällen die Lichtbilder kurzfristig auszuleihen und im Fachkommissariat (z. B. Betrugskommissariat) aufzubewahren mit der Maßgabe, bei jeder Entnahme schriftlich zu dokumentieren, wer wann was entnommen hat und wo das Lichtbild während der Leihe aufbewahrt wird. Einzelne Polizeibehörden favorisieren die Verfahrensweise, Lichtbildvorlagen nur im Fachkommissariat durchzuführen, um eine Ausleihe von vornherein zu unterbinden.

Zur Vereinheitlichung der Praxis auf einem angemessenen Datenschutzniveau hält der LfD es für ratsam, landeseinheitlich zu regeln, wie der Nachweis für aus KpS und aus Lichtbildsammlungen entnommene Lichtbilder zu führen ist.

5.17 Veröffentlichung einer unzutreffenden Presseerklärung im Internet

Gegen den Beschwerdeführer wurde auf der Basis eines richterlichen Beschlusses wegen Vergehens nach dem Tierschutzgesetz eine Hausdurchsuchung durchgeführt, die zum Ziel hatte, das mögliche Tatwerkzeug (ein Luftgewehr) aufzufinden und zu beschlagnahmen. Diese Durchsuchung wurde in Abwesenheit des Betroffenen durchgeführt. Am Tag darauf veröffentlichte die Polizei darüber folgende Pressemeldung:

„X-Dorf: Falsche Warnung vor dem Hund

Im Rahmen der Durchsuchungsmaßnahmen in den Landkreisen x und y (wir berichteten) sollte am Donnerstagmorgen auch die Wohnung eines Mannes in X-Dorf durchsucht werden. Die Eingangstür wurde jedoch von einem Riesenschnauzer bewacht, der außerordentlich aggressiv an die Tür sprang und bellte. Ein Holzschild verkündete, dass er schon eine Vielzahl von Einbrechern, Postboten, Katzen und Autoreifen zur Strecke gebracht hätte. Sicherheitshalber riefen die Beamten eine Streife der Diensthundestaffel, die dann die Tür öffnete. Auf der Stelle verlor der Hund sämtliche ihm zugeschriebenen Qualitäten und flüchtete verängstigt bis in die hintere Ecke des Geländes. Die Durchsuchungsmaßnahmen konnten fortgeführt werden.“

Die Presseerklärung, auf die im vorstehenden Text Bezug genommen wurde, war zwei Tage vorher von der Polizei veröffentlicht worden und hatte folgenden Inhalt:

„Landkreis x und y: Durchsuchungen wegen BTM

Am Mittwoch ab 6.00 Uhr durchsuchte die Polizei in Zusammenarbeit mit den Staatsanwaltschaften x und y die Wohnungen von 17 Männern und Frauen, denen nach mehrmonatigen Ermittlungen Verstöße gegen das Betäubungsmittelgesetz zur Last gelegt werden. Betroffen waren Anwesen in A-Dorf, B-Bach und C-Stadt. Die Kripo wurde unterstützt durch Bereitschaftspolizei, Diensthundeführer und SEK. Die 17 Beschuldigten im Alter von 18 bis 38 Jahren sind teilweise als Konsumenten, teilweise als Kleindealer von BTM in Erscheinung getreten. Es konnten im Laufe der Durchsuchungsmaßnahmen bei fast jeder dieser Personen kleine Mengen Betäubungsmittel und Utensilien wie Haschischpfeifen etc. sichergestellt werden. Bei einem 29-jährigen Beschuldigten wurden u. a. 50 Schuss Munition sichergestellt. In B-Bach wurde bei einem 21-jährigen Mann zudem eine Pumpgun gefunden.“

Beide Pressemitteilungen wurden unter „www.polizei.rlp.de, Pressemitteilungen“, in das Internet eingestellt. Die örtliche Tageszeitung veröffentlichte einen Artikel, in dem der Text der ersten vorstehenden polizeilichen Pressemitteilung weitgehend wörtlich übernommen worden ist. Der Beschwerdeführer erhob eine Dienstaufsichtsbeschwerde wegen des Inhaltes der ihn betreffenden Pressemeldung.

Das Polizeipräsidium beschied ihn folgendermaßen:

„Hinsichtlich der Pressemeldung vom ..... ist bedauerlicherweise ein Zusammenhang zwischen einer größeren Durchsuchungsaktion am vorangegangenen Mittwoch und der bei Ihnen stattgefundenen Durchsuchung hergestellt worden, der nicht besteht. Wir bedauern dies ausdrücklich."

Der Beschwerdeführer erhob weitere Dienstaufsichtsbeschwerde beim Ministerium des Innern und für Sport, das ihm Folgendes mitteilte:

„Danach hat das Polizeipräsidium Ihnen gegenüber den Fehler eingeräumt und bedauert, in unzutreffender Weise in der Pressemeldung einen Zusammenhang mit einer anderen Durchsuchungsmaßnahme hergestellt zu haben. Damit hat es sich bei Ihnen ausdrücklich entschuldigt. Ich halte diese Entschuldigung für angemessen und sehe aufgrund des zu Recht eingestandenen Fehlers von hier aus keinen weiteren Handlungsbedarf."

Die den Beschwerdeführer betreffende Pressemitteilung war im Internet-Angebot der rheinland-pfälzischen Polizei noch nach ca. acht Monaten abrufbar. Das der Pressemitteilung zugrunde liegende Strafverfahren gegen den Betroffenen war zwischenzeitlich schon eingestellt worden.

Nunmehr hat das Ministerium des Innern und für Sport gegenüber dem Polizeipräsidium auf folgende Gesichtspunkte hingewiesen: Die ursprüngliche Presseerklärung über die Durchsuchung beim Betroffenen sei unzureichend anonymisiert gewesen. Die Darstellung sei geeignet gewesen, den Betroffenen verächtlich zu machen. Die fehlerhafte Presseerklärung sei acht Monate unverändert im Internet veröffentlicht worden. Eine behördliche Richtigstellung der fehlerhaften Pressemitteilung sei nicht erfolgt. Es sei dafür Sorge zu tragen, dass bei der Pressearbeit des Polizeipräsidiums künftig solche Fehler nicht mehr auftreten.

Der LfD hat aus datenschutzrechtlicher Sicht begrüßt, dass das Ministerium des Innern und für Sport damit letztlich doch die gebotenen Folgerungen aus dem hier vorliegenden Sachverhalt gezogen hat.

5.18 Missbräuchliche Nutzung des Kfz-Zulassungsregisters

Eine Petentin berichtete von einer unzulässigen Datenabfrage aus dem Kfz-Zulassungsregister. Wie im Strafverfahren festgestellt, tätigte ein Polizeibeamter auf Veranlassung einer Polizeiverwaltungsangestellten den unzulässigen Datenabruf. Zur Verdeutlichung der Bedeutung des Datenschutzes bei der Nutzung automatisierter Abrufsysteme und der Verhinderung künftiger Datenmissbräuche durch die betroffene Polizeibehörde hatte der LfD die Prüfung disziplinarrechtlicher Schritte gegen den Polizeibeamten und dienstaufsichtliche Maßnahmen gegen die Verwaltungsangestellte angeregt. Die Behördenleitung folgte der Anregung des LfD und sprach dem Polizeibeamten eine deutliche Missbilligung aus. Das festgestellte Fehlverhalten der Verwaltungsangestellten wurde ausdrücklich beanstandet.

5.19 Vollzugshilfeersuchen anderer Bundesländer zur Erlangung von Material für DNA-Untersuchungen

Die Anfrage eines Petenten veranlasste den LfD, nachfolgende Problemstellung mit dem Ministerium des Innern und für Sport zu erörtern:

Eine rheinland-pfälzische Polizeidienststelle wurde von einer Polizeibehörde eines anderen Bundeslandes ersucht, den wegen einer gefährlichen Körperverletzung zu einer Freiheitsstrafe (zur Bewährung ausgesetzt) verurteilten und in Rheinland-Pfalz wohnhaften Petenten zur Abgabe einer Speichelprobe zwecks Durchführung einer DNA-Untersuchung zu veranlassen.

Zur Abgabe der Speichelprobe wurde der Petent von der Polizei Rheinland-Pfalz mit dem Vordruck „Vorladung – Original-POLRP 3001/2001" vorgeladen. Ergänzend war zum Zweck der Vorladung „Sonstige Gründe, Abgabe einer Speichelprobe" und die sachbearbeitende Dienststelle der Polizei des anderen Bundeslandes angegeben. Da es sich um ein Standardformular zur anlassunabhängigen Vorladung von Personen handelt, enthält der Vordruck keinerlei Informationen zu den gesetzlichen Voraussetzungen, zum Zweck der Maßnahme, zur Einverständniserklärung und zur Datenspeicherung bei der Entnahme und Untersuchung von Speichelproben.

Aus Sicht des LfD ist die Polizei verpflichtet, den Betroffenen auch auf sein Untersuchungsverweigerungsrecht hinzuweisen (Rechtsgedanke des § 52 Abs. 3 StPO). Da in Rheinland-Pfalz solche Untersuchungen ausschließlich auf der Grundlage richterlicher Entscheidungen durchgeführt werden, tritt die aufgezeigte Problematik lediglich im Rahmen von Vollzugshilfeersuchen der Länderpolizeien auf, bei denen sich die polizeiliche Praxis hinsichtlich der Durchführung molekulargenetischer Untersuchungen bei verurteilten Straftätern unterscheidet. Beispielsweise in Bayern und in Baden-Württemberg werden zunächst auf der Basis der Freiwilligkeit Speichelproben entnommen, um sie molekulargenetisch untersuchen zu lassen. In diesen Fällen hält der LfD es zumindest für wünschenswert, dass die ersuchende Polizeidienststelle ihre entsprechenden Vordrucke zur Entnahme einer Speichelprobe bzw. der Einwilligungserklärung dem Ersuchen beifügt, damit die rheinland-pfälzische Polizei diesen Vordruck dann in ihrer Vorladung an den Betroffenen weitergeben könnte. Diese Anregung des LfD nahm das Ministerium des Innern und für Sport zum Anlass, das LKA mit der Umsetzung folgender Verfahrensweise zu beauftragen, gegen die keine datenschutzrechtlichen Bedenken mehr bestehen:

Das LKA Rheinland-Pfalz bittet die Landeskriminalämter anderer Bundesländer, ihre Polizeidienststellen darauf hinzuweisen, dass bei Amtshilfeersuchen an rheinland-pfälzische Polizeidienststellen eine umfassende Belehrung über die gesetzlichen Grundlagen sowie die Darstellung des Umfanges der Maßnahmen (Probenentnahme, Untersuchung, Speicherung der Daten) und eine Einverständniserklärung künftig beizufügen sind. Der von der Maßnahme Betroffene erhält die Unterlagen mit der Vorladung zugestellt. Amtshilfeersuchen ohne beigefügte Unterlagen kann damit künftig nicht mehr entsprochen werden.

5.20 Zulässigkeit anlassloser, regelmäßiger Übermittlung von Tagesberichten an ausländische Streitkräfte

Das Auskunftsersuchen eines bDSB, ob das Zusenden von Tagesberichten einer Polizeibehörde an in der Bundesrepublik Deutschland stationierte Streitkräfte gegen datenschutzrechtliche Vorschriften verstoße, beantwortete der LfD wie folgt:

Für die Übermittlung personenbezogener Daten an ausländische Stellen zu repressiven Zwecken sind die Regelungen des Abkommens zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen (NATO-Truppenstatut) und dem Zusatzabkommen zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen (NTS-ZA) einschlägig. Die Rechtslage in Bezug auf die Übermittlung personenbezogener Daten zu präventivpolizeilichen Zwecken wurde im Rundbrief des Ministeriums des Innern und für Sport an die polizeiliche Praxis vom 21. Januar 1998 dargelegt. Danach ist eine Übermittlung nur zur Bekämpfung von Straftaten sowie Ordnungswidrigkeiten oder zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit zulässig. Da die Erforderlichkeit bei der Übermittlung von Geschädigten- bzw. Opferdaten anhand von regelmäßig übersandten Tagesberichten zur sachgerechten und umfassenden Aufgabenerledigung der Streitkräfte nicht nachvollziehbar dargelegt werden konnte, kam der LfD zu dem Ergebnis, dass die zur Rede stehende anlasslose, regelmäßige Übersendung von Tagesberichten, die personenbezogene Daten enthalten, insbesondere auch die Übermittlung von Geschädigten- bzw. Opferdaten, nicht zulässig ist.

Die Polizeibehörden haben diese Auffassung akzeptiert.

5.21 Extranet der Polizei EXTRAPOL

Die Polizeien des Bundes und der Länder betreiben seit 1. Januar 2001 ein überwiegend dezentral aufgebautes Netzwerk, über das Fachinformationen zur Polizeiarbeit zur Verfügung gestellt werden (Enzyklopädie polizeilichen Wissens; Leitfäden, Presseinformationen, Newsticker etc.). Dabei handelt es sich im Wesentlichen um ein Portal, das nur für die Polizei zur Verfügung gestellt wird. Rheinland-Pfalz hat dabei die organisatorische Federführung übernommen.

Datenschutzrechtlich interessant ist dieses Projekt deshalb, weil auch personenbezogene Daten darüber verbreitet werden. Derzeit sind dies zwar nur Fahndungsdaten, die im Bereich der Polizei ohnehin allgemein ohne Einschränkung zur Verfügung stehen; geplant ist aber eine Erweiterung auf Lagebilder, wobei dann auch Personen (Gefährder, Verantwortliche) benannt werden sollen.

In Rheinland-Pfalz verfügen alle der ca. 5 000 Arbeitsstationen über einen Zugang. EXTRAPOL basiert auf Web-Technologien und ist als geschlossenes Netz konzipiert. Betrieben wird es über das Corporate Network der Polizeien (CNP), eine ausschließlich von der Polizei genutzte Leitungsstruktur; auf der oberen Netzebene des CNP erfolgt standardmäßig eine Verschlüsselung. Jedes teilnehmende Land hält die von ihm betreuten Inhalte lokal vor und stellt diese über entsprechende Links, in Ausnahmefällen auch als Kopie, zur Verfügung. Den Zugang zu EXTRAPOL eröffnet ein gemeinsames Portal; dieses wird durch Rheinland-Pfalz beim LDI betrieben (Extranet-Portalserver). Das BKA ist gegenwärtig dabei, die technische Infrastruktur für eine Kommunikation im Extranet aufzubauen (Nachrichtengruppen, Diskussionsforen etc.).

EXTRAPOL basiert damit auf einer verteilten Datenhaltung in den Ländern bzw. beim Bund; das Portal eröffnet lediglich eine „Sicht“ auf vorhandene Informationen. Die redaktionelle Verantwortung für die jeweiligen Inhalte, die Dauer der Einstellung und die Datenpflege liegt bei den Ländern bzw. dem Bund. Gepflegt werden die Inhalte über ein Redaktionssystem (Content Management System CMS); hier besteht die Möglichkeit, das zentral auf dem Portalserver angebotene CMS oder eine jeweilige landeseigene Lösung zu nutzen. Im Normalfall verfügt jedes Land über eine Stelle, welche die Einstellung vornimmt und die Qualitätssicherung gewährleistet (Datenkonsistenz, Einstellungsfristen, Wiedervorlagefristen, Zugriffssteuerung). Eine beim BKA angesiedelte Fachredaktion nimmt koordinierende Aufgaben wahr.

Soweit Informationen bereitgestellt werden, stehen diese grundsätzlich bundesweit zur Verfügung. Eine automatische Datenübernahme (Import) aus polizeilichen Verfahren erfolgt gegenwärtig nicht.

Die laufenden Planungen sehen eine Erweiterung von EXTRAPOL um eine „Ereignisübersicht“ vor. In dieser sollen den Lagezentren der Länder Informationen und Hinweise zu bestimmten Ereignissen zur Verfügung gestellt werden (Jahrestage, Großveranstaltungen, bedeutsame Festnahmen u. a. m.). Die Ereignisdatenbank soll insoweit die gegenwärtige Fernschreib- und Telefax-Kommunikation ersetzen. Jedes Lagezentrum kann einerseits selbständig Ereignisse einstellen und andererseits zu einem vorhandenen Ereignis Zusatzinformationen bereitstellen und diese mit vorhandenen Einträgen verknüpfen (z. B. Stadionpläne, Anfahrtskizzen, nähere Beschreibungen usw.). Zugriffsmöglichkeiten sind im Rahmen einer geschlossenen Benutzergruppe ausschließlich für die Mitarbeiter der Lagezentren (in Rheinland-Pfalz ca. 20) vorgesehen.

Aus rechtlicher Sicht erscheinen bezüglich dieser Pilot-Nutzung derzeit folgende Datenschutzfragen relevant:

– Wird der Erforderlichkeitsgrundsatz in allen Fällen beachtet? Insbesondere: Haben alle eingestellten Meldungen überregionalen Bezug? Solange eine regionale Beschränkung der Zugriffe auf die Informationen nicht möglich ist, dürfen Informationen von bloß regionaler Bedeutung mit Personenbezug nicht bundesweit verbreitet werden.

– Liegt eine zentrale Datenspeicherung vor, für die eine ausdrückliche Rechtsgrundlage erforderlich ist? Diese Sicht der Dinge wird nach Auffassung des LfD dem Verfahren nicht gerecht: Jedes Land bleibt für die von ihm eingestellten Daten verantwortlich und kann auch die Löschung jederzeit veranlassen bzw. selbst durchführen.

– Handelt es sich um Auftragsdatenverarbeitung? In diesem Fall wäre Auftragnehmer wohl das Land Rheinland-Pfalz, Auftraggeber wären die übrigen Projektbeteiligten. Oder handelt es sich um 17 datenverarbeitende Stellen, die jeweils Online-Zugriffe auf eigene Datenbestände eröffnen? Aus der Sicht des LfD liegt eine Mischform, je nach eingesetzter Technik, vor: Eröffnung eines Online-Verfahrens dann, wenn auf im Landessystem gespeicherte Daten über den Server der rheinland-pfälzischen Polizei nur der Zugriff eröffnet wird; Auftragsdatenverarbeitung dann, wenn eine Datenspeicherung auf dem ausgelagerten Server erfolgt.

– Wer hat nach welchem Recht für das Verfahren eine Errichtungsanordnung zu erstellen? Aus Sicht der Datenschutzbeauftragten hat dies das jeweilige beteiligte Bundesland nach seinem Polizeirecht zu tun.

Auf der Grundlage der vorhandenen Möglichkeiten des Redaktionssystems hat der LfD in technischer Hinsicht folgende Empfehlungen ausgesprochen:

– Festlegung möglicher Ereignisarten und der für diese zu meldenden Informationen,

– Strukturierung der Inhalte über Eingabemasken im Redaktionssystem,

– Aufnahme von Metadaten, anhand derer der Zeitpunkt der Einstellung und die verantwortliche Dienststelle, Autor etc. erkennbar sind,

– Schaffung von Möglichkeiten für eine Befristung der Einstellung bzw. die Vergabe von Wiedervorlagefristen,

– Einrichtung von Mechanismen, die eine Steuerung und ggf. Beschränkung der Zugriffsmöglichkeiten erlauben.

Zum weiteren Funktionsumfang des Redaktionssystems, insbesondere zu den Möglichkeiten der Benutzerverwaltung und der Nachvollziehbarkeit von Einträgen und Abfragen, sind örtliche Feststellungen vorgesehen.

6. Verfassungsschutz

6.1 Änderung des Landesverfassungsschutzgesetzes

6.1.1 Rechtslage im Bund und im Land

Im Terrorismusbekämpfungsgesetz des Bundes (am 1. Januar 2002 in Kraft getreten: Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002, BGBl. I S. 361) wurden den Nachrichtendiensten des Bundes neue Befugnisse eingeräumt (s.Tz. 2.4). Es wurden u. a. das Bundesverfassungsschutzgesetz, das BND-Gesetz und das MAD-Gesetz geändert. Im Einzelnen handelt es sich um folgende neue Bestimmungen:

– Auskunftsrechte gegenüber Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen über Konten, Kontoinhaber sowie hinsichtlich Geldbewegungen und Geldanlagen (§ 8 Abs. 5 BVerfSchG; § 2 Abs. 1 a BNDG)

– Auskunftsrechte gegenüber Postdienstleistern über Namen, Anschriften, Postfächer und sonstige Umstände des Postverkehrs (§ 8 Abs. 6 BVerfSchG)

– Auskunftsrechte gegenüber Luftfahrtunternehmen über Namen, Anschriften und Inanspruchnahme von Transportleistungen und sonstige Umstände des Luftverkehrs (§ 8 Abs. 7 BVerfSchG)

– Auskunftsrechte gegenüber Telekommunikationsdienstleistern und Teledienstleistern über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten (§ 8 Abs. 8 BVerfSchG; § 10 Abs. 3 MADG; § 8 Abs. 3 a BNDG)

– Einsatz technischer Mittel (sog. IMSI-Catcher) zur Ermittlung der Identität und des Standorts aktiv geschalteter Mobiltelefone (§ 9 Abs. 4 BVerfSchG). Im Rahmen dieser Gesetzesänderungen wurden auch die Kontrollrechte des Parlamentarischen Kontrollgremiums und der G 10-Kommission auf die neu eingefügten Befugnisse der Sicherheitsbehörden erweitert.

In der Folge dieser Regelungen ist auch das Landesverfassungsschutzgesetz geändert worden (mit Gesetz vom 16. Dezember 2002, GVBl. S. 477). Es sind insbesondere die im Bundesrecht eingeführten neuen Auskunftspflichten für Geldinstitute, Postdienstleistungs- und Luftverkehrsunternehmen gegenüber dem Landesverfassungsschutz übernommen worden. Die Änderungen betreffen insbesondere die §§ 10 a, 14 und 21 LVerfSchG.

Die neuen Befugnisse unterliegen – in Erfüllung eines wesentlichen Anliegens des LfD – einer Erfolgskontrolle und Befristung; nach Art. 4 Abs. 2 des Änderungsgesetzes vom 16. Dezember 2002, GVBl. S. 477, treten diese Vorschriften mit dem 10. Januar 2007 außer Kraft; falls sie sich bewährt haben sollten, müsste die Befristung durch einen Gesetzesbeschluss des Landtags aufgehoben werden.

6.1.2 Erkenntnisse über den praktischen Einsatz der neuen Befugnisse

Erkenntnisse über die praktischen Auswirkungen dieser Regelungen, wie sie sich für den Bundesbereich aus dem Bericht des Parlamentarischen Kontrollgremiums des Deutschen Bundestages vom 12. Mai 2003 an den Bundestag ergeben (Bundestagsdrucksache 15/981), liegen dem LfD für den Landesbereich derzeit noch nicht vor.

Nach dem genannten Bericht stellt sich die Situation auf der Ebene des Bundes wie folgt dar:

6.1.2.1 Auskunftsersuchen der Nachrichtendienste

Im Berichtszeitraum, dem 1. Januar 2002 bis zum 31. Dezember 2002, stellte das BfV insgesamt sechs Auskunftsersuchen an Kreditinstitute. Die Auskunftsersuchen richteten sich gegen sechs Personen, die im Verdacht standen, Mitglied in einer ausländischen extremistischen Vereinigung zu sein oder eine solche zu unterstützen.

Der BND stellte ein Auskunftsersuchen mit drei Teilanträgen an drei verschiedene Geldinstitute. Die Maßnahmen richteten sich gegen drei Personen, die im Verdacht der Finanzierung des internationalen Terrorismus und der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung standen. Ziel der Auskunftsersuchen war die Ermittlung von Konten und Kontoinhabern bei deutschen Banken. Bei Postdienstleistern wurden durch das BfV keine Auskunftsersuchen gestellt.

An ein Luftfahrtunternehmen wurde lediglich ein Auskunftsersuchen gestellt, das darauf gerichtet war, Informationen zur Identifikation einer Person zu erlangen. Es war eine Person betroffen, die im Verdacht stand, Verbindungen zu einer terroristischen Vereinigung zu unterhalten und an der Planung von terroristischen Anschlägen beteiligt zu sein.

Von BfV, MAD und BND wurden insgesamt 17 Auskunftsersuchen an Telekommunikationsunternehmen und Teledienstleister gestellt. Die Verfahren richteten sich gegen 18 Hauptbetroffene. Im Einzelnen: Das BfV hat im Berichtszeitraum 13 Auskunftsersuchen beantragt und vollzogen. Diese Maßnahmen richteten sich gegen 13 Personen, die im Verdacht standen, einer ausländischen extremistischen Vereinigung anzugehören, sich an der Planung von terroristischen Anschlägen zu beteiligen oder für einen fremden Nachrichtendienst tätig zu sein. Aufgrund der Auskunftsersuchen konnten Verbindungs- und Standortdaten des Mobilfunkanschlusses aktiv geschalteter Endgeräte, Verbindungsdaten zu versandten und empfangenen E-Mails und Erkenntnisse über die Reiseaktivitäten der Betroffenen erlangt werden.

Seitens des MAD wurden zwei Auskunftsersuchen an Teledienstleister gestellt. Diese Maßnahmen richteten sich unmittelbar gegen zwei Angehörige der Bundeswehr. In einem Fall stand der Hauptbetroffene im Verdacht, für einen fremden Nachrichtendienst tätig zu sein. Das zweite Auskunftsersuchen richtete sich gegen ein mutmaßliches Mitglied einer terroristischen Vereinigung.

Der BND richtete zwei Auskunftsersuchen an Telekommunikationsunternehmen. Die Maßnahmen wurden zur Abwehr internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland durchgeführt. Die Auskunftsersuchen bezogen sich auf drei Personen mit sieben Anschlussnummern und waren an vier verschiedene Telekommunikationsdienstleister gerichtet. Mit den durch die Auskünfte gewonnenen Informationen sollte durch den Abgleich der Verbindungsdaten festgestellt werden, ob die Anschlussinhaber in Deutschland in regelmäßigem Kontakt zu mutmaßlichen Mitgliedern terroristischer Vereinigungen stehen oder ob die ermittelten weiteren Telekommunikationsanschlüsse möglicherweise von terroristischen Vereinigungen genutzt werden.

6.1.2.2 Einsatz des sog. IMSI-Catchers

Für einen ordnungsgemäßen Antrag auf Anordnung einer Telekommunikationsüberwachung nach dem G 10-Gesetz ist die Benennung einer Telefonnummer erforderlich. Angehörige terroristischer Gruppen nutzen allerdings zunehmend Mobiltelefone, deren Herkunft den Sicherheitsbehörden nicht bekannt ist. Die Telefonnummern solcher Geräte können deshalb auch über den Betreiber nicht festgestellt werden. Mit Hilfe der Kartennummer lässt sich allerdings in der Regel die dazugehörige Telefonnummer problemlos ermitteln. Daher wurde in § 9 Abs. 4 BVerfSchG eine gesetzliche Ermächtigung zum Einsatz des sog. „IMSI-Catchers“ zur Ermittlung der Geräte- und Kartennummern von Telefonen und auf dieser Basis auch zur Lokalisierung des Standortes des Gerätes aufgenommen. Mit dem sog. „IMSI-Catcher“ ist es möglich, die IMSI (International Mobile Subscriber Identity) eines eingeschalteten Handys in seinem Einzugsbereich zu ermitteln. Diese IMSI ist eine weltweit einmalige Kennung, die den Vertrags-

partner eines Netzbetreibers eindeutig identifiziert. Die IMSI ist auf der sog. SIM-Karte (SIM = Subscriber Identity Module) gespeichert, die ein Mobilfunkteilnehmer bei Abschluss eines Vertrages erhält. Mit Hilfe der IMSI kann nicht nur die Identität des Teilnehmers, sondern auch dessen Mobilfunktelefonnummer bestimmt werden. Zur Ermittlung der IMSI simuliert ein „IMSI-Catcher" die Basisstation einer regulären Funkzelle eines Mobilfunknetzes. Eingeschaltete Handys im Einzugbereich dieser „vermeintlichen" Basisstation mit einer SIM des simulierten Netzbetreibers buchen sich nun automatisch beim IMSI-Catcher ein. Durch einen speziellen „IMSI-Request" der Basisstation – einen Befehl, der sonst üblicherweise nur im Fehlerfall benötigt wird – wird die Herausgabe der IMSI vom Handy erzwungen. Ist der von einer observierten Person genutzte Netzbetreiber nicht bekannt, muss diese Suche ggf. für Basisstationen aller Netzbetreiber durchgeführt werden. In Funkzellen mit vielen Teilnehmern kann es zudem erforderlich sein, mehrere Messungen durchzuführen, bis die gesuchte IMSI aus der Vielzahl gesammelter Daten herausgefiltert werden kann. Da durch den Einsatz eines IMSI-Catchers aus technischen Gründen regelmäßig auch Daten Dritter erhoben werden, sind hier besonders hohe Anforderungen an die Verhältnismäßigkeit der Maßnahme zu stellen. Der Einsatz ist nur zulässig, wenn ohne ihn die Erreichung des Zwecks der Überwachungsmaßnahme aussichtslos oder wesentlich erschwert wäre. Die erhobenen Daten Dritter unterliegen einem absoluten Verwertungsverbot.

Im Berichtszeitraum kam der IMSI-Catcher dreimal zum Einsatz. Die Maßnahmen richteten sich gegen drei Personen, die entweder im Verdacht standen, Mitglied oder Unterstützer einer ausländischen extremistischen Vereinigung zu sein oder einer terroristischen Vereinigung anzugehören.

6.1.3 Bewertung

Mit den durch das Terrorismusbekämpfungsgesetz den Sicherheitsdiensten neu übertragenen Befugnissen wird in den Schutzbereich des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 GG, Art. 14 LV) und in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG, Art. 4 a LV) eingegriffen. Den deutschen Nachrichtendiensten, den beteiligten Ministerien und den sie kontrollierenden Gremien kommt insofern eine große Verantwortung bei der Beantragung, Genehmigung und Durchführung jeder einzelnen Anordnung zu. Aus der Sicht des Parlamentarischen Kontrollgremiums des Bundes hat sich auch im Bereich der neuen Befugnisse der Nachrichtendienste der Eindruck bestätigt, dass sich die Sicherheitsbehörden dieser Verantwortung bewusst sind, ihre Tätigkeit gewissenhaft ausüben und die Beschränkungen der Bürgerinnen und Bürger gerade auch auf diesem Gebiet so gering wie möglich halten.

Eine fundierte, abschließende Bewertung war dem Parlamentarischen Kontrollgremium des Bundes allerdings ein Jahr nach In-Kraft-Treten der neuen Regelungen angesichts der bislang noch relativ geringen Zahl von insgesamt dreißig durchgeführten Maßnahmen nicht möglich. Diese Evaluierung soll in den in den kommenden Jahren folgenden Berichten erfolgen.

Es ist davon auszugehen, dass auch der rheinland-pfälzische Verfassungsschutz die neuen Instrumente in vergleichbar zurückhaltender Weise nutzen wird. Der LfD wird die Entwicklung in diesem Bereich weiter aufmerksam beobachten.

6.2 Neue Regelungen im Sicherheitsüberprüfungsgesetz

Wie in das Bundesgesetz wurde auch in das Landessicherheitsüberprüfungsgesetz der vorbeugende personelle Sabotageschutz eingeführt. Dies geht über den bisherigen Anwendungsbereich des SÜG, also den personellen Geheimschutz, hinaus. Um den Kreis der von solchen weit reichenden Überprüfungsmaßnahmen betroffenen Personen und Bereichen der Wirtschaft und des öffentlichen Dienstes einzugrenzen, war zu fordern, nach dem Bestimmtheitsgrundsatz die Voraussetzungen für die betroffenen sicherheitsempfindlichen Stellen im Gesetz selbst zu definieren. Der Gesetzgeber ist dieser Forderung auf der Ebene des Bundes gefolgt; die Regelungen zum vorbeugenden Sabotageschutz sind normenklar gefasst worden. Der Landesgesetzgeber hat sich dem in den §§ 1, 2, 4, 10, 21, 24, 25, 27 und 31 LSÜG angeschlossen. Die neuen Befugnisse unterliegen ebenfalls – in Erfüllung eines wesentlichen Anliegens des LfD – einer Erfolgskontrolle und Befristung; nach Art. 4 Abs. 2 des Änderungsgesetzes vom 16. Dezember 2002, GVBl. S. 477, treten diese Vorschriften mit dem 10. Januar 2007 außer Kraft. Zu Einzelheiten der Bundesregelung wird auf den 19. Tb. des BfD, Tz. 20.1, verwiesen.

6.3 Auskunftsantrag an den Landesverfassungsschutz

Auf seinen Auskunftsantrag an den Landesverfassungsschutz über die zu seiner Person bei der Verfassungsschutzbehörde gespeicherten Daten wurde einem Petenten mitgeteilt, die Auskunft könne wegen der andernfalls bestehenden Gefährdung der Aufgabenerfüllung des Verfassungsschutzes nicht erteilt werden. Deshalb bat der Petent den LfD, die Rechtmäßigkeit der Datenspeicherungen sowie der Auskunftsverweigerung des Verfassungsschutzes zu überprüfen.

Diese Prüfung wurde vorgenommen mit dem Ergebnis, dass die beim Verfassungsschutz über den Petenten vorhandenen Erkenntnisse rechtmäßig erhoben und gespeichert waren. Sie wurden an keine Stelle außerhalb des Verfassungsschutzes weitergegeben. Rechte des Petenten sind nicht verletzt worden.

Vor dem Hintergrund der nunmehr aufgrund seiner Schreiben und der persönlichen Vorsprache des Petenten beim LfD vorliegenden weiteren Informationen wurden die ihn betreffenden Erkenntnisse in einer Datei des Verfassungsschutzes gelöscht. Damit konnte dem Anliegen des Petenten umfassend Rechnung getragen werden.

7. Justiz

7.1 Allgemeine Datenschutzfragen

7.1.1 Elektronische Gerichtsaktenführung; Justizkommunikationsgesetz

Das Bundesministerium der Justiz hat einen Gesetzentwurf vorgelegt, nach dem die Einführung der elektronischen Aktenführung und der Auskunftserteilung aus Akten durch Direktzugriffsverfahren beabsichtigt ist. Danach soll auch für viele Fälle das Internet (insbesondere die Website des elektronischen Bundesanzeigers) als Medium gerichtlicher Veröffentlichungen vorgesehen werden.

Der LfD hat auf folgende Gesichtspunkte hingewiesen, die aus seiner Sicht bei der weiteren Beratung des Gesetzentwurfs berücksichtigt werden sollten:

Die Anerkennung der Echtheit von Dokumenten setzt nach dem Entwurf im Allgemeinen den Einsatz der qualifizierten elektronischen Signatur mit dauerhaft überprüfbarem Zertifikat voraus. Dies ist zu begrüßen und sollte aufrechterhalten bleiben. Insbesondere Behörden sollten insoweit vorbildlich sein und eigene Dokumente nach Möglichkeit in dieser Form qualifiziert signieren (vgl. Beschluss der DSB-Konferenz vom 27. März 2003, Anlage 20). Im Entwurf zu § 110 a Abs. 1 Nr. 1 c OwiG sind vom Gebot der dauerhaften Überprüfbarkeit von Signaturen Ausnahmen vorgesehen: Die Bundesregierung und die Landesregierungen können danach für ihren jeweiligen Zuständigkeitsbereich durch Rechtsverordnung zulassen, dass bei der Signierung von Dokumenten der Verwaltungsbehörde nach § 110 b Abs. 1 und 2 die Signatur nicht auf einem Zertifikat beruhen muss, das dauerhaft überprüfbar ist. Für diese Ausnahmeregelungen werden keine Kriterien genannt. Sie sollten nur in Betracht gezogen werden, wenn wegen der Eigenart der betroffenen Vorgänge von Aufbewahrungsfristen auszugehen ist, die eine längerfristige Überprüfbarkeit entbehrlich machen.

Die zentralen Vorschriften zur elektronischen Aktenführung (§§ 298 a ZPO, 55 b VwGO, 52 b FGO, 65 b SGG, 56 d ArbGG, 110 a OwiG) enthalten zu datenschutzrechtlich wesentlichen Fragen keine Aussagen. So fehlen beispielsweise Regelungen zu

- der Pflicht zur verschlüsselten Datenspeicherung;
- Vorgaben zur Archivierbarkeit elektronisch geführter Akten;
- Vorgaben zu Zugriffsschranken, die strikt am Erforderlichkeitsgrundsatz zu orientieren sind;
- Vorgaben zu sonstigen technisch-organisatorischen Datenschutzmaßnahmen wie Protokollierungen von Veränderungen und Zugriffen etc.;
- Pflichten datenabrufender Stellen zur Beachtung von Zweckbindungen und Löschungsvorgaben;
- der Beschränkung der Auftragsdatenverarbeitung auf besonders vertrauenswürdige Stellen unter Wahrung des Grundsatzes der Unabhängigkeit der Justiz.

Die in allen betroffenen Prozessordnungen vorgesehenen Verordnungsermächtigungen sprechen nicht an, welche Punkte genau mit welchem wesentlichen Inhalt jeweils durch den Verordnungsgeber (die Landesregierungen) geregelt werden sollen. Auch die Begründung enthält insoweit keine Hinweise. Es erscheint zudem problematisch, eine Zersplitterung der Rechtslage für solche Vorgaben zu ermöglichen, die für den Grundrechtsschutz der Betroffenen und für die Unabhängigkeit der Rechtspflege wesentlich sind. Soweit § 110 a Abs. 2 OwiG-Entwurf weitergehende Einzelheiten des Inhalts einer entsprechenden Rechtsverordnung nennt, ist dies grundsätzlich zu begrüßen; es fehlt aber auch hier ein Hinweis auf solche Regelungen, die aus datenschutzrechtlicher Sicht wesentlich wären (vgl. die obigen Beispiele).

Falls davon ausgegangen werden sollte, dass ergänzend zu den Verfahrensordnungen und den auf technische Vorgaben begrenzten Rechtsverordnungen die allgemeinen Datenschutzgesetze angewendet werden sollten, wäre dies eine denkbare Lösung. Allerdings sollte dann zumindest in der Begründung zum Ausdruck kommen, dass ergänzend die allgemeinen Datenschutzgesetze heranzuziehen sind.

Besonders bedeutsam aus datenschutzrechtlicher Sicht sind auch die Vorschriften, die eine Veröffentlichung von Daten im Internet erlauben oder vorsehen. Die Entwurfsregelungen über gerichtliche Veröffentlichungen im Internet sind zahlreich: §§ 187 ZPO (öffentliche Zustellung), 948 Abs. 1 ZPO (öffentliche Bekanntmachung im Aufgebotsverfahren), 956 ZPO (öffentliche Bekanntmachung des Ausschlussurteils im Aufgebotsverfahren), 1017 Abs. 2 ZPO (öffentliche Bekanntmachung eines Ausschlussurteils bei Kraftloserklärung einer Urkunde), 1020 Satz 3 ZPO (öffentliche Bekanntmachung einer Zahlungssperre im Aufgebotsverfahren), 1022 Abs. 1 Satz 3 ZPO (öffentliche Bekanntmachung der Aufhebung der Zahlungssperre), §§ 56 a Abs. 2 VwGO (öffentliche Bekanntmachungen aller Art in Verfahren mit mehr als 50 Beteiligten), 65 Abs. 3 VwGO (öffentliche Aufforderung zur Anmeldung in Verfahren mit mehr als 50 beiladungsfähigen Personen), § 60 a FGO (öffentliche Aufforderung zur Anmeldung in Verfahren mit mehr als 50 beiladungsfähigen Personen), § 75 Abs. 2 a SGG (öffentliche Aufforderung zur Anmeldung in Verfahren mit mehr als 20 beiladungsfähigen Personen), §§ 12, 30, 52, 58 und 75 GmbHG. In diesen Vorschriften wird dabei jeweils der elektronische Bundesanzeiger als Veröffentlichungsmedium genannt.

Die hierzu gegebenen Begründungen sind unzureichend. Es wird regelmäßig nur erklärt, die Informationen würden in ein allgemein, also auch international zugängliches Informationssystem eingestellt, das von der interessierten Öffentlichkeit genutzt werden könne. Die derzeitige Veröffentlichung im (Print)-Bundesanzeiger werde tatsächlich nur von einem eingeschränkten Leserkreis zur Kenntnis genommen.

Es bedürfte jedoch unter Geltung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes und des Gebots des geringstmöglichen zur Zweckerfüllung ausreichenden Grundrechtseingriffs in jedem einzelnen Fall der Darlegung, warum eine internationale Öffentlichkeit dem jeweiligen Ziel der Veröffentlichung entspricht und am ehesten gerecht wird. In jedem Fall wären auch die möglicherweise für die Betroffenen einhergehenden Nachteile einer Internet-Veröffentlichung (insbesondere mangelnder Schutz gegen zweckändernde dauerhafte Nutzung der Daten im Internet durch Dritte, die an keine Verwendungsschranken gebunden sind) dagegen abzuwägen. Zu berücksichtigen ist, dass mit der Einführung des elektronischen Bundesanzeigers (www.ebundesanzeiger. de) durch das Transparenz- und Publizitätsgesetz von 2002 für die Unternehmensmitteilungen bei der Aktiengesellschaft kein allgemeiner Anlass für Folgeänderungen außerhalb des Unternehmensrechts geschaffen wurde. Zudem sollten mindestens die Anforderungen, die durch § 9 Abs. 2 Insolvenzordnung an die Internet-Veröffentlichung von Schuldnerdaten geschaffen wurden, auch für sonstige Internet-Veröffentlichungen gelten.

Dem § 948 Abs. 1 und dem § 1009 ZPO soll jeweils folgender Satz angefügt werden:

„Zusätzlich kann die öffentliche Bekanntmachung in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem erfolgen." Die Ergänzung soll die zusätzliche Möglichkeit einer öffentlichen Bekanntmachung in Aufgebotsverfahren insbesondere durch Einstellung ins Internet auf der Homepage des jeweiligen Gerichts schaffen. Damit solle ein mittlerweile weit verbreitetes Medium genutzt werden, um eine zeitgemäße Möglichkeit der Kenntnisnahme des Aufgebots zu schaffen. Auch hier gilt die Anregung, zumindest § 9 Abs. 2 InsolvenzO inhaltlich zu übernehmen.

In diesem Zusammenhang ist darauf hinzuweisen, dass die Begründung zu § 56 a Abs. 2 VwGO eine Aussage enthält, die aus Datenschutzsicht nicht akzeptabel ist; danach bleibe es einem Gericht unbenommen, die dort genannten Informationen auch auf die eigene Homepage einzustellen. Nach Auffassung des LfD bedürfte die Veröffentlichung personenbezogener Daten im Internet durch ein Gericht in jedem Fall einer dies ausdrücklich legitimierenden gesetzlichen Grundlage.

Die oben genannten Bestimmungen über die Einführung der elektronischen Aktenführung differieren u. a. in der Frage, ob durch den Verordnungsgeber den Gerichten die Einführung der elektronischen Akte vorzugeben ist (so §§ 55 b VwGO, 52 b FGO, 65 b SGG) oder ob der Verordnungsgeber den Gerichten (bzw. den Bußgeldbehörden) insoweit ein Ermessen einräumen kann (so §§ 298 a ZPO, 56 d ArbGG, 110 a OwiG). Ein Maßstab für dieses Ermessen und ein Grund für diese Differenzierung sind nicht ersichtlich.

In diesen Normen fällt weiterhin eine unterschiedliche Begriffsverwendung auf, deren Grund nicht ersichtlich ist: Zum Teil wird von Aufbewahrung der elektronischen Akten gesprochen (§§ 298 a ZPO, 56 d ArbGG), zum Teil von Verwahrung dieser Akten (§§ 55 b VwGO, 52 b FGO, 65 b SGG). Falls kein sachlicher Unterschied zwischen Aufbewahrung und Verwahrung bestehen sollte (wovon ich ausgehe), sollte der Gesetzgeber einen einheitlichen Begriff verwenden.

Für das OwiG-Verfahren wird ausdrücklich die Möglichkeit vorgesehen, Akteneinsicht an Verfahrensbeteiligte im Wege des Direktabrufs zu gewähren (§ 110 e Abs. 1 Satz 2 OWiG-E); es werden besondere technische und organisatorische Sicherungsmaßnahmen vorgesehen. Die Regelungen der anderen Prozessordnungen sind diesbezüglich nicht so klar: § 299 Abs. 3 Satz 1 ZPO-E spricht davon, Akteneinsicht könne u. a. durch „Bereitstellung von elektronischen Dokumenten" gewährt werden. Ob darunter auch die Bereitstellung im Rahmen eines Direktabrufverfahrens zu verstehen ist, wird auch aus der Begründung nicht deutlich. Aus Datenschutzsicht sind im Falle eines Direktabrufverfahrens mindestens die Gesichtspunkte gesetzlich zu regeln, die in § 110 e OwiG-E genannt sind (hierzu gehören – neben anderen besonderen technischen Sicherungsmaßnahmen – insbesondere auch angemessene Protokollierungen der Zugriffe). Vergleichbares gilt für § 100 Abs. 2 VwGO-E, § 78 Abs. 2 FGO-E und § 120 Abs. 2 SGG-E. Hier ist ausdrücklich von einem elektronischen Zugriff auf den Akteninhalt durch Beteiligte die Rede. Die Regelung der hierfür erforderlichen besonderen Datenschutzmaßnahmen erfolgt jedoch nicht bzw. nur unzureichend.

Der LfD wird den Fortgang des Gesetzgebungsverfahrens weiterhin aufmerksam begleiten; damit werden langwirkende Grundsätze für „E-Government" in der Justiz geschaffen, deren Bedeutung kaum überschätzt werden kann.

7.1.2 Zum Gerichtsaktenaufbewahrungsgesetz

Das Bundesministerium der Justiz hat den Entwurf eines Gerichtsaktenaufbewahrungsgesetzes vorgelegt. Dieses Gesetz soll einem seit langem vorgebrachten Petitum der Datenschutzbeauftragten des Bundes und der Länder Rechnung tragen, wonach die Aufbewahrung von Gerichtsakten in der Justiz nach Beendigung des gerichtlichen Verfahrens einer gesetzlichen Grundlage bedarf. Der Entwurf soll die grundsätzlichen Voraussetzungen für die weitere Aufbewahrung von Gerichtsakten regeln und die Länder ermächtigen, die konkrete Dauer der Aufbewahrungsfristen durch Rechtsverordnung in genereller Form selbst zu bestimmen. Maßgeblich für die Dauer der Aufbewahrung soll der Zweck der Aufbewahrung unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes sein.

Dieser Gesetzentwurf ist im Grundsatz sehr zu begrüßen. Seine Regelungsdichte ist allerdings gering; die Maßstäbe für die Verordnungsgeber können als vage bezeichnet werden. Mindestens folgende Gesichtspunkte sollten aus der Sicht des LfD noch Eingang in den Entwurf finden:

– Der Verordnungsgeber sollte aufgefordert werden, insbesondere im Fall der elektronischen Aktenführung bei der Regelung von Speicherfristen zwischen unterschiedlichen Zwecken dienenden Aktenteilen oder solchen unterschiedlicher Sensitivität unter dem Gesichtspunkt der Datensparsamkeit zu differenzieren: Urteile sind länger aufzuheben als Aktenbestandteile, die nur temporären Zwecken dienen.

– Auch der Antrag Betroffener auf Vernichtung von Akten oder Aktenteilen sollte als Prüfungsanlass vorgesehen werden.

– Falls eine Löschung besonders sensitiver Aktenbestandteile wegen überwiegender Dokumentationszwecke nicht in Betracht kommt, sollten Sperrungsregelungen vorgesehen werden.

– Nach § 2 Abs. 2 Satz 2 Nr. 3 des Entwurfs sollen berechtigte Interessen von Nichtverfahrensbeteiligten ausreichen, die Aufbewahrungsfristen über die für die Verfahrensbeteiligten bestehenden Erfordernisse hinaus zu verlängern. Dies ist aus datenschutzrechtlicher Sicht kein ausreichendes Kriterium. Für die Auskunfterteilung an Nichtverfahrensbeteiligte wird in den Verfahrensordnungen regelmäßig ein rechtliches Interesse gefordert (z. B. § 299 Abs. 3 ZPO). Darauf sollte auch die Regelung der Aufbewahrungsfristen abstellen.

Es bleibt zu hoffen, dass der Gesetzentwurf mit den vorgenannten Änderungen rasch verabschiedet werden wird.

7.1.3 Internet-Veröffentlichungen der Gerichte

Im Gerichtsorganisationsgesetz des Landes wurde die Vorschrift, wonach Veröffentlichungen im Staatsanzeiger zu erfolgen haben, durch die Vorschrift ersetzt, dass die Veröffentlichung im Internet zu erfolgen hat, wenn die Veröffentlichung (gesetzlich, im Justizbereich regelmäßig also in einem Bundesgesetz) „in einem Bekanntmachungsblatt oder in einem elektronischen Informationssystem“ vorgeschrieben ist.

Damit wird ein Automatismus vorgeschrieben: Unabhängig von der Sensitivität der Daten, unabhängig von den besonderen Gefährdungen der Internet-Veröffentlichung (weltweite Verbreitung, Unkontrollierbarkeit der Speicherdauer – keine effiziente Löschungsmöglichkeit –, einfache Recherchemöglichkeiten, damit Vervielfachung der Missbrauchsgefahren) wird für alle bundesgesetzlich „in einem elektronischen Informationssystem“ ermöglichten Veröffentlichungen die Internet-Veröffentlichung vorgesehen.

Es ist allerdings davon auszugehen, dass die zugrunde liegenden bundesgesetzlichen Regelungen jeweils die näheren Modalitäten bestimmen und auch die datenschutzrechtlich zu fordernden Einschränkungen regeln. Der Begriff des „elektronischen Informationssystems“ wurde vom Bundesgesetzgeber bislang ausschließlich verwandt, um das Internet zu bezeichnen. Lokale „elektronische Informationssysteme“ sind damit regelmäßig nicht gemeint.

Fest steht, dass die besonderen Bedingungen der Internet-Veröffentlichungen bei der Entscheidung, ob dieses Medium genutzt wird, eine Rolle zu spielen haben. Da allerdings der Bundesgesetzgeber diese Entscheidung im Justizbereich zu treffen hat und das Gerichtsorganisationsgesetz des Landes eine bloße technische Umsetzungsregelung für andernorts getroffene Entscheidungen darstellt, konnte datenschutzrechtlich nichts dagegen eingewandt werden.

In der Praxis sind derartige Veröffentlichungen vom Bundesgesetzgeber bereits im Insolvenzverfahren vorgesehen (Rechtsverordnung zu öffentlichen Bekanntmachungen im Insolvenzverfahren im Internet vom 12. Februar 2002, BGBl. I S. 677); eine Ausweitung auf andere Bereiche (insbesondere das Zwangsversteigerungsverfahren) ist zu erwarten. Der LfD hat hier gemeinsam mit anderen Datenschutzbeauftragten vom Bundesgesetzgeber insbesondere Vorkehrungen gefordert, die das Kopieren solcher Daten erschweren. Nur dann kann auch davon ausgegangen werden, dass die vorgesehenen Löschungsfristen auch praktisch Auswirkungen haben. Die Landesregierung (das Ministerium der Justiz) hat diese Forderungen gegenüber dem Bund dankenswerterweise unterstützt und zu ihrer gesetzlichen Verankerung auf der Ebene des Bundes beigetragen.

Offen in diesem Zusammenhang ist beispielsweise noch die Frage, ob die Nennung des Eigentümernamens im Internet bei der Zwangsversteigerung wirklich in allen Fällen erforderlich ist und ob Dritte, die Daten aus Veröffentlichungen (auch aus Printmedien) entnehmen und selbständig im Internet veröffentlichen, nicht gesetzlich zur Löschung entsprechend den für gerichtliche Veröffentlichungen geltenden Fristen verpflichtet werden sollten.

Angesichts der vielfältigen Missbrauchsmöglichkeiten der hier in Rede stehenden Daten wird der LfD diesen Bereich weiter aufmerksam beobachten.

7.1.4 Angabe des Geburtsdatums im Adressfeld bei förmlichen Zustellungen

Ein Bürger fühlte sich dadurch in seinen Rechten beeinträchtigt, dass ein Gerichtsvollzieher sein Geburtsdatum in das Adressfeld eines an ihn gerichteten Schreibens aufgenommen hatte. Der LfD war der Auffassung, dass dafür grundsätzlich keine Notwendigkeit bestehe. In seiner Stellungnahme allerdings trug der Gerichtsvollzieher eine Reihe von Argumenten für die von ihm verfolgte Verfahrensweise vor. Dies veranlasste den LfD, das Ministerium der Justiz seinerseits zur Prüfung der entstandenen Fragen aufzufordern. Daraufhin wurden die OLG-Präsidenten befragt, um die Praxis und die dort bestehenden Auffassungen kennen zu lernen.

Im Ergebnis hat das Ministerium folgende Auffassung geäußert:

Der Vermerk des Geburtsdatums des Zustellungsempfängers im Adressfeld sei nur dann zulässig, wenn dies erforderlich sei, um eine Zustellung an den richtigen Empfänger zu gewährleisten. Diese Voraussetzung werde regelmäßig erfüllt sein, wenn Namensgleichheiten unter der Adresse des Empfängers bekannt seien oder wenn bereits Zustellversuche wegen Identifizierungsschwierigkeiten fehlgeschlagen seien. In allen anderen Fällen habe also eine Angabe des Geburtsdatums im Adressfeld grundsätzlich zu unterbleiben.

Mit diesem Inhalt sind die Gerichtsvollzieher des Landes auch unterrichtet worden. Der LfD begrüßt die auf dieser Auffassung beruhende Handlungsempfehlung an die Gerichtsvollzieher.

7.1.5 Datenübermittlungen durch Gerichte anlässlich der Einholung von Gutachten zur Verhandlungsfähigkeit

Anlässlich einer Eingabe, für deren konkrete Bearbeitung der LfD nicht zuständig war, ist er auf die in der Überschrift genannte Frage gestoßen. Die auslösende Eingabe betraf folgenden Sachverhalt:

Die Beschwerdeführerin war wegen Betruges angeklagt. Sie blieb wiederholt unter Berufung auf Krankheit den anberaumten Terminen zur mündlichen Verhandlung fern. Daraufhin ordnete der Vorsitzende Richter die Untersuchung durch einen medizinischen Sachverständigen an (er beauftragte das örtliche Gesundheitsamt). Zur Vorbereitung ließ er diesem die vollständigen bis dahin entstandenen Verfahrensakten, einschließlich der Anklageschrift, zukommen. Auf Einwendungen der Angeklagten gegen dieses Verfahren bemerkte er u. a., dieses entspreche einer landesweiten Übung.

Der LfD hat der Beschwerdeführerin mitgeteilt, dass der Vorsitzende Richter vorliegend eine richterliche Handlung vorgenommen habe, die in den Bereich der richterlichen Unabhängigkeit falle; er könne jedenfalls den konkreten Sachverhalt nicht bewerten.

Unabhängig von dem konkreten Einzelfall (der möglicherweise deshalb auch spezielle Fragen aufwarf, weil der vorgeworfene Betrug unter Einbeziehung des Gesundheitsamts begangen worden sein soll), hatte der LfD den Eindruck, dass hier eine allgemeine Verfahrensweise bei den Gerichten bestehen könnte, die aus datenschutzrechtlicher Sicht thematisiert werden sollte.

Es stellt sich die Frage, ob es für einen medizinischen Gutachter zur Beurteilung der Verhandlungsfähigkeit wirklich erforderlich ist, Kenntnis von dem Stand der Ermittlungen gegen den Betroffenen zu erhalten (oder, in anderen Gerichtszweigen, Informationen über den Streitgegenstand im Einzelnen). Würde es nicht ausreichen (und der Sache eher dienen), wenn dem Gutachter – außer dem konkreten Anlass des Untersuchungsauftrags – lediglich mitgeteilt würde, welche zeitliche und sonstige Belastung des zu Untersuchenden durch das weitere Verfahren jeweils zu erwarten ist?

Der LfD wandte sich deshalb an das Ministerium der Justiz. Ihm war bewusst, dass auch das Ministerium hier keine konkreten Weisungen veranlassen kann. Er hat dieses jedoch über den Vorgang unterrichtet und gebeten mitzuteilen, ob es eine Möglichkeit sehe, diese Fragen gelegentlich im Kreis der Richterschaft mit dem Ziel zu erörtern, den berechtigten Belangen der Betroffenen stärker als bisher gerecht zu werden. Das Ministerium hat zugesichert, in diesem Sinn tätig werden zu wollen.

7.1.6 Pressemeldungen von Gerichten

Ein Aids-Hilfe-Verein hat den LfD auf eine Presseveröffentlichung eines Verwaltungsgerichts in einem Asylverfahren mit der Überschrift „Kranker Asylbewerber darf vorerst bleiben“ aufmerksam gemacht. Seiner Ansicht nach wurde durch diese Veröffentlichung der Datenschutz des Betroffenen verletzt: Zwar wurde sein Name nicht genannt; sein kleines afrikanisches Herkunftsland aber sei ausdrücklich erwähnt worden; außerdem wohne er in einer überschaubaren Gemeinde in einem ebenfalls genannten rheinland-pfälzischen Landkreis. Viele Mitbürger würden ihn kennen und aus den Angaben im Presseartikel wieder erkennen. Dadurch wüssten sie nun über seine Aids-Erkrankung Bescheid; er sei nach Erscheinen des Artikels darauf sogar angesprochen worden. Außerdem würden sie jetzt Informationen über seine aufenthaltsrechtliche Situation und seine Verfolgung in seiner Heimat erhalten haben.

Die Informationen dieses Artikels stammten aus einer Pressemeldung des entscheidenden Verwaltungsgerichts, die im Internet-Angebot des Gerichts unter „Pressemitteilungen“ abrufbar war. Vor diesem Hintergrund hat der LfD das Gericht um Stellungnahme gebeten, ob die Veröffentlichungen in der genannten Pressemitteilung den Vorgaben der Verwaltungsvorschrift des Ministeriums der Justiz zur „Tätigkeit der Justizpressestellen“ vom 16. Oktober 1997, JBl. 97, S. 485 ff., entsprechen würde. Insbesondere hatte der LfD Zweifel, ob die Ziff. 6.2 dieser VV ausreichend beachtet wurde, wonach keine personenbezogenen Angaben in Pressemitteilungen gemacht werden dürfen, die einzelne Personen bestimmbar machen.

Das Gericht hat wie folgt Stellung genommen:

Es habe nicht damit gerechnet, dass aus den Angaben in der Pressemitteilung, die sehr allgemein gewesen seien, ein Rückschluss auf eine konkrete Person möglich sein könnte. Es bedauerte, dass es offensichtlich entgegen seiner Erwartung doch zur Reidentifizierung des Betroffenen gekommen sei. In künftigen Fällen werde man noch mehr darauf bedacht sein, jede Personenbeziehbarkeit auszuschließen.

Der LfD geht davon aus, dass damit die Sensibilität für das Problem deutlich erhöht wurde und dass sich vergleichbare Fälle in Zukunft nicht wiederholen werden.

7.2 Zivilrecht

7.2.1 Elektronisches Grundbuch Rheinland-Pfalz: datenschutzrechtliche Chancen und Risiken

Das automatisiert geführte Grundbuch ist in Rheinland-Pfalz inzwischen nahezu flächendeckend eingeführt. Die Bereitschaft des Ministeriums der Justiz, aber auch des für die Zulassung zum elektronischen Abrufverfahren auf das Grundbuch landesweit zuständigen OLG Zweibrücken zur umfassenden Information des LfD ist als ausgesprochen positiv hervorzuheben.

Die Automation bietet generell im Bereich des Grundbuchs zwar Chancen, sie begründet aber auch neue Risiken. Für die erste Alternative steht die Möglichkeit, Grundbuchauszüge so zu gestalten, dass sie auf das für den Einsichtbegehrenden Wesentliche reduziert sind. Insoweit hat das Ministerium der Justiz Vorschläge des LfD positiv aufgenommen. Das Ministerium stimmt mit dem LfD überein, dass im herkömmlichen Verfahren Auszüge aus dem Grundbuch so weit wie möglich auf den Umfang zu beschränken sind, der durch das vorgetragene berechtigte Interesse begrenzt wird. Künftig ist aufgrund der Umgestaltung des automatisierten Grundbuchs zur Datenbankanwendung mit Änderungen zu rechnen, die die Verwirklichung dieses Anliegens noch in einem weiteren Umfang möglich machen. Dies ist ausgesprochen erfreulich.

Für die Begründung von neuen Risiken ist das Direktabrufverfahren von Grundbuchdaten durch Dritte als Beispiel zu nennen. Derzeit können Kommunen – von der kleinen Verbandsgemeinde bis zur Großstadt – eine Vielzahl von Terminals einrichten, von denen aus die Mitarbeiter einen technisch uneingeschränkten Zugriff auf alle Grundbuchblätter im Land – künftig sogar bundesweit – haben. Unter den derzeitigen Bedingungen wird nicht protokolliert, welcher Bedienstete zu welcher Zeit auf welches Grundbuchblatt zugegriffen hat: Die Protokollierung beschränkt sich darauf, den Zugriff der Gebietskörperschaft zu erfassen. Welche Stelle und welche Person innerhalb der Stadt oder Gemeinde zugegriffen haben, bleibt unklar. Eine effektive Prüfung, ob missbräuchliche Zugriffe erfolgt sind, scheint dem LfD damit – jedenfalls dann, wenn die abrufende Kommune über zahlreiche Abrufterminals verfügt – kaum möglich zu sein.

Das Ministerium der Justiz ist – in Übereinstimmung mit den Justizverwaltungen aller anderen Bundesländer – der Auffassung, derzeit bestehe kein zwingender Änderungsbedarf. Aus folgenden Gründen kann der LfD dieser Bewertung nicht folgen:

1. Auch die Grundbucheinsicht von Behörden hängt vom Vorliegen eines berechtigten Interesses in jedem Einzelfall ab; darin besteht Übereinstimmung mit dem Ministerium der Justiz.

2. Dass beim automatisierten Abrufverfahren in allen Fällen, auch in denen des Abrufs durch Behörden, eine nachträgliche Überprüfung des Vorliegens eines berechtigten Interesses für jeden einzelnen getätigten Abruf durch die zuständige Aufsichtsbehörde möglich sein muss, ergibt sich eindeutig aus § 83 Abs. 1 GBV. Daraus ergibt sich auch, dass zu diesem Zweck eine geeignete Protokollierung vorhanden sein muss.

3. Die Regelung des § 82 GBV, die nur von einer Kennung spricht, steht dem nicht entgegen. Diese Vorgabe ist keinesfalls als erschöpfende und abschließende Regelung über den Inhalt der vorzusehenden Protokollierung zu verstehen. Sie regelt vielmehr nur eine erforderliche besondere technische Datenschutzmaßnahme zur Abwehr missbräuchlicher externer Zugriffsversuche auf den Datenbestand des automatisierten Grundbuchs. Diese Regelung hat mit Fragen des Inhalts von Protokollierungen und zu diesem Zweck zu vergebenden Identitätsmerkmalen nichts zu tun.

4. Vor dem Hintergrund des derzeit landesweiten und künftig sogar bundesweiten Zugriffs und der genannten unzureichenden Protokollierungen fehlt es aus der Sicht des LfD in Anbetracht der schutzwürdigen Belange der Grundstückseigentümer und der sonstigen Betroffenen an der Angemessenheit des automatisierten Zugriffsverfahrens durch die Gemeinden. Die Voraussetzungen des § 133 Abs. 1 Nr. 1 GBO liegen unter diesem Aspekt nicht vor.

5. Gerade weil eine erteilte Erlaubnis nach § 133 Abs. 7 GBO tendenziell bundesweite Wirkung hätte und den Zugriff auf den Datenbestand aller Grundbuchämter bundesweit erlauben würde (was derzeit nur aus technischen Gründen noch nicht realisiert ist), wäre das Vorliegen dieser Voraussetzung besonders intensiv unter Berücksichtigung dieser Reichweite der Zulassung zu prüfen. Es ist kaum vorstellbar, dass auch nur eine rheinland-pfälzische Gemeinde unter diesen Bedingungen plausibel geltend machen könnte, ihre berechtigten Interessen forderten den bundesweiten Grundbuchzugriff.

6. In den zugrunde liegenden Verwaltungsvereinbarungen zwischen dem Land und den Gemeinden werden die jeweiligen Zwecke der beabsichtigten Zugriffe auf das Grundbuch nicht genügend klargestellt.

7. Nicht nur der LfD, auch andere Datenschutzbeauftragte beurteilen die Sach- und Rechtslage gleichermaßen. Der sächsische Datenschutzbeauftragte z. B. hat im Hinblick auf die hier erörterte Situation in seinem Tätigkeitsbericht von 1999 u. a. ausgeführt:

   „Umso bedauerlicher ist es, dass aufgrund der zurzeit eingesetzten Technik das vom Gesetz gebotene Datenschutzniveau nicht eingehalten wird . .. Angesichts dieser erheblichen datenschutztechnischen Defizite werde ich mich auch weiterhin für eine Ausgestaltung des EDV-Grundbuchs einsetzen, die den Vorgaben der GBO und der GBV entspricht."

Vor diesem Hintergrund bemüht sich auch der LfD weiterhin um eine Änderung der technischen Bedingungen des Direktzugriffs auf das automatisierte Grundbuch. Dies ist auf der Ebene des Landes aber auch deshalb schwierig, weil die Systementwicklung im bundesweiten Verbund erfolgt und ein allgemeines Problembewusstsein aller Beteiligten noch nicht besteht. Das Ministerium der Justiz hat signalisiert, dass es das datenschutzrechtliche Anliegen grundsätzlich für nachvollziehbar hält, dass – in Übereinstimmung mit den Justizressorts der anderen Bundesländer – aus seiner Sicht allerdings die gesetzlichen Regelungen auch das derzeitige Verfahren zulassen.

7.2.2 Internet-Veröffentlichung von Wertgutachten bei Grundstücks-Zwangsversteigerungen

Die in Schleswig-Holstein ansässige Firma Hansen Marketing betreibt das Internet-Angebot www.hanmark.de als „Dienstleister für Amtsgerichte" und veröffentlicht dort Zwangsversteigerungstermine mit den zugehörigen Wertgutachten für Gebäude und Grundstücke. Nach der im Internet zugänglichen Liste nutzen derzeit dreizehn rheinland-pfälzische Amtsgerichte diesen Service, aber auch eine Reihe von Amtsgerichten der Länder Baden-Württemberg, Hessen, Nordrhein-Westfalen, Saarland und Schleswig-Holstein sind vertreten.

Der LfD geht davon aus, dass weder aus §§ 39, 40 noch aus § 42 ZVG die Befugnis für die Vollstreckungsgerichte resultiert, Wertgutachten im Internet zu veröffentlichen. § 39 ZVG betrifft allein die Veröffentlichung der Terminbestimmung; darüber hinausgehende Informationen über die Zwangsversteigerung werden von § 42 ZVG speziell geregelt. Danach steht zwar jedem ein Akteneinsichtsrecht ohne jede nähere Begründung zu; Voraussetzung dieses Rechts ist aber zumindest eine Antragstellung. Keinesfalls ist von dieser Bestimmung die Befugnis zur Veröffentlichung umfasst: Schon eine Veröffentlichung des Inhalts der Akten in einem herkömmlichen Publikationsorgan käme danach nicht in Betracht, noch weniger aber eine entsprechende Internet-Veröffentlichung, die mit besonderen Gefahren für die Betroffenen verbunden ist.

Vor dem Hintergrund der Besonderheiten bei Internet-Veröffentlichungen hat der Gesetzgeber die entsprechende Veröffentlichung von Insolvenzdaten genau und unter einschränkenden Bedingungen geregelt (§ 9 Abs. 2 InsO). Diese Regelung war erforderlich, um Internet-Veröffentlichungen in diesem Bereich zuzulassen; sie ist für diesen Bereich als abschließend anzusehen (vgl. die Stellungnahme des BMJ in der Bundestagsdrucksache 15/181 vom 12. Dezember 2002).

Soweit die Auffassung vertreten wird, vorliegend handele es sich nicht um personenbeziehbare Daten, kann sich der LfD dem nicht anschließen. Aus seiner Sicht sind die im Internet-Angebot www.hanmark.de veröffentlichten Informationen „personenbezogene Daten" im Sinne des Datenschutzrechts. Zwar werden der Name und die Anschrift von Schuldner und Eigentümer der betroffenen Liegenschaften nicht veröffentlicht. Die Angaben über das betroffene Grundstück sind aber so genau (Flurstück, häufig auch Straße und Hausnummer, außerdem Fotos der Außenansicht), dass für einen beliebig großen Personenkreis durch einfach zu erlangende Zusatzinformationen (häufig durch einen Blick in das Telefonbuch) Bewohner und auch Eigentümer der Liegenschaften zu eruieren sind. Damit greifen die gesetzlichen Schranken für den Umgang öffentlicher Stellen mit personenbezogenen Daten ein.

Das Ministerium der Justiz hat die Bedenken des LfD für nicht durchgreifend erklärt. Von dessen Argumentation ist der LfD allerdings nicht überzeugt. Er bemüht sich derzeit um eine bundesweite Abstimmung unter den Datenschutzbeauftragten, um entweder eine bundesgesetzliche Rechtsgrundlage für diese Vorgehensweise oder eine Änderung der Veröffentlichungspraxis zu erreichen. Wenn eine solche Gesetzesänderung nicht erfolgen sollte, wäre aus seiner Sicht zumindest die Einwilligung der Betroffenen vor einer solchen Veröffentlichung einzuholen.

7.3 Strafrecht, Strafverfahrensrecht

7.3.1 Eurojust

Zwischenzeitlich hat sich die europäische Eurojust-Behörde (s. 18. Tb., Tz. 7.12.2) in Den Haag etabliert. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer 62. Konferenz am 25./26. Oktober 2001 einen Beschluss gefasst, in dem sie ihre Anforderungen an die für diese Stelle erforderlichen Rechtsgrundlagen sowie die Tätigkeit dieser Behörde formuliert haben (vgl. Anlage 2).

Auf der europäischen Ebene entspricht der Eurojust-Beschluss des Rates weitgehend diesen Anforderungen (vom 28. Februar 2002, ABl. EG Nr. L 63, 6. März 2002, S. 1). Inzwischen hat die Bundesregierung einen Gesetzentwurf in den Bundestag eingebracht, um die gesetzlichen Voraussetzungen dafür zu schaffen, dass die deutschen Staatsanwaltschaften Daten von Verdächtigen bzw. Beschuldigten an Eurojust übermitteln dürfen (Entwurf eines Eurojust-Gesetzes vom 15. August 2003, Bundestagsdrucksache 545/03).

Die Datenschutzbeauftragten haben in unterschiedlichem Umfang Änderungswünsche an dieses Gesetz formuliert; die vom LfD geforderten Klarstellungen, die vom BfD unterstützt worden sind, haben Eingang in den Gesetzentwurf gefunden.

Zu prüfen bleibt, ob die Kontrollinstitutionen für Eurojust wirksam arbeiten werden und ob die berechtigten Ansprüche Betroffener auf fairen Umgang mit ihren Daten und insbesondere auf Auskunft – wenn dies die Ermittlungsverfahren nicht hindert – effektiv erfüllt werden. An diesen Feststellungen wird sich der LfD im Rahmen seiner Möglichkeiten gemeinsam mit den anderen Datenschutzbeauftragten, insbesondere mit dem Bundesdatenschutzbeauftragten, beteiligen.

Es ist zu erwarten, dass Eurojust – entsprechend den Ankündigungen von maßgeblichen europäischen und nationalen Stellen – nur eine Vorstufe für den allseits geforderten europäischen Staatsanwalt sein wird. Die mit einer solchen Institution verbundenen Probleme sind vielfältig; ihr gegenüber ist insbesondere eine wirksame justitielle Kontrolle zu fordern. Das für Eurojust gefundene Modell einer speziellen unabhängigen Kontrollkommission wird angesichts der für den europäischen Staatsanwalt zu erwartenden erheblichen Eingriffsbefugnisse (z. B. Durchsuchung, vorläufige Sicherungs- und Aufklärungsmaßnahmen etc.) nicht ausreichen.

7.3.2 Probleme der Telekommunikationsüberwachung

Die TKÜ steht aus verschiedenen Gründen besonders intensiv im Blickfeld der Datenschutzbeauftragten: Diese eingreifende Maßnahme in das Datenschutzgrundrecht und das Telekommunikationsgeheimnis nimmt zahlenmäßig – jedenfalls insgesamt, im Bundesdurchschnitt – zu. Auf der Ebene des Landes ist der Zuwachs allerdings eher moderat.

Zweifelhaft ist bzw. war, ob der Erfolg dieser Maßnahmen es rechtfertigt, in diesem Umfang in Grundrechte der Bürger einzugreifen. Hierzu hat die inzwischen vorliegende Studie des Max-Planck-Instituts für Strafrecht, die auch veröffentlicht wurde und jedermann zugänglich ist, tragfähige Erkenntnisse geliefert. Die Datenschutzbeauftragten haben das Ergebnis dieser Studie mit der in der Anlage 27 beigefügten Entschließung gewürdigt.

Aber auch die Weiterentwicklung der Technik ist eine Ursache für das zunehmende Unbehagen der Datenschutzbeauftragten: IMSI-Catcher und SMS-Blaster (Tz. 7.3.3) lassen aus dem Handy einen Peilsender werden, der ständig Standortinformationen über den Nutzer liefert.

Schließlich sind in diesem Zusammenhang die Bestrebungen der Sicherheitsbehörden auf europäischer und nationaler Ebene zu erwähnen, die Verbindungsdaten aller Nutzer von modernen Kommunikationsmitteln auf Vorrat – für den Fall, dass sie zur Strafverfolgung benötigt werden – durch die TK-Dienstleister speichern zu lassen. Dagegen haben sich sowohl die Konferenz der europäischen Datenschutzbeauftragten wie die des Bundes und der Länder entschieden gewandt (vgl. Anlage 12; Entschließung vom 24./25. Oktober 2002, Zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet).

Der LfD bemüht sich gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder weiterhin um eine tragfähige Balance zwischen Grundrechten und staatlichen Befugnissen, die in immer neuen Diskussionen und Auseinandersetzungen herzustellen ist (s. auch oben Tz. 5.1 zur geplanten Verankerung der TKÜ im Polizeirecht).

7.3.3 SMS-Blaster: Neue Wege der Handy-Ortung

Die Länderpolizeien sowie der BGS nutzen seit ca. einem Jahr die Möglichkeit, über sog. „stille SMS“ Positionsmeldungen aktiver Mobiltelefone zu erzeugen und zu erfassen, wenn eine Telekommuniaktionsabhörmaßnahme gem. § 100 a StPO angeordnet und durchgeführt wird. Die Rückmeldung erfolgt ohne Zutun und Kenntnis des Handy-Besitzers. Der Versand der SMS wird über Provider, die einen entsprechenden SMS-Server betreiben, vorgenommen.

Die Aufforderung zur Standortmeldung kann automatisch periodisch wiederholt werden, um bei aktivem Mobiltelefon ein Bewegungsprofil zu bilden. Weiterhin besteht die Möglichkeit, die Anfrage bei vorübergehend nicht erreichbaren Mobiltelefonen in eine Warteschleife zu stellen. Die Nutzung der Stealth-Ping-Funktion ist an eine Registrierung beim Betreiber des SMS-Servers gebunden.

Die (stille) Entgegennahme der Nachricht durch das Mobiltelefon stellt eine Aktivität dar, die im Rahmen einer laufenden TÜ-Maßnahme erfasst wird. Der damit erzeugte S-Record enthält neben den Verbindungsangaben die Kennung der aktuellen Funkzelle und die Geokoordinaten von deren Sendeanlage (Basisstation).

Unabhängig davon sieht das SNPP-Protokoll vor, dass auf das PING-Kommando hin eine Rückantwort an den SMS-Server erfolgt, ebenfalls mit Standortangaben. Um welche Informationen es sich dabei konkret handelt, inwieweit und für welchen Zeitraum diese bei dem in Anspruch genommenen Serverbetreiber gespeichert werden, ist gegenwärtig nicht bekannt. Die Polizei verarbeitet die Rückantwort auf das PING-Kommando bislang nur insoweit, als erkennbar wird, ob eine SMS überhaupt zugestellt werden konnte. Der Versand einer stillen SMS wird mit Datum, Uhrzeit und Anschlussnummer im Journal der eingesetzten Client-Software protokolliert.

In welchem Umfang beim Betreiber des Stealth-Ping-Service personenbezogene Informationen gespeichert werden, welche Zugriffsmöglichkeiten bestehen und wann dort eine Löschung der Einträge erfolgt, ist gegenwärtig nicht bekannt und soll geklärt werden.

Diese und die weiteren oben als ungeklärt bezeichneten Fragen sind derzeit auch im Kreise der Datenschutzbeauftragten des Bundes und der Länder noch offen. Sie könnten wohl nur im Zusammenwirken mit den hier am Markt tätigen Providern geklärt werden.

Der LfD bemüht sich weiter um eine Klärung der angesprochenen Fragen.

7.3.4 Beschlagnahme der gesamten Mandantendaten eines Steuerberaters

Eine Bürgerin hat sich mit folgendem Vorbringen an den LfD gewandt:

Gegen ihren Steuerberater werde ein Strafverfahren durchgeführt. Dessen Gegenstand sei, dass er Scheinrechnungen ausgestellt habe, die er an drei namentlich bekannte andere Personen gegen Entgelt weitergegeben habe. Diese hätten dann die Scheinrechnungen in ihre Steuererklärungen aufgenommen. Sie selbst gehöre nicht zu den Betroffenen dieses Strafverfahrens.

Im Zuge des Verfahrens erging ein amtsgerichtlicher Durchsuchungsbeschluss. Darin wurde der für die Strafverfolgung relevante Sachverhalt konkret geschildert; es wurde die Durchsuchung der Praxis des Steuerberaters zur Auffindung nachstehender Beweismittel angeordnet: „Scheinrechnungen, Buchhaltungsunterlagen der anderweitig verfolgten drei Personen, Unterlagen, Kontounterlagen."

Im Verlauf der Durchsuchung hat die Staatsanwaltschaft dann sämtliche EDV-Speicher des Steuerberaters kopiert bzw. mitgenommen. Zu diesen Daten gehörten auch die steuerlichen Informationen über die Beschwerdeführerin. Sie war in keiner Weise von dem Strafverfahren betroffen. Sie erklärte, sie halte es für rechtswidrig, dass nicht nur die Daten der vom Strafverfahren betroffenen Personen, sondern auch ihre Daten und die aller anderen Mandanten des Steuerberaters durch die Strafverfolgungsbehörden zur Kenntnis genommen wurden.

Die Staatsanwaltschaft hat dazu ausgeführt, die umfassende Datensicherung sei notwendig gewesen, da aufgrund des Umfangs der Daten eine ausgewählte Datensicherung bezüglich der konkret Beschuldigten in den Kanzleiräumen nicht möglich gewesen sei. Anschließend seien die Daten an Amtsstelle gesichtet und nur, soweit für das Verfahren beweiserheblich, ausgedruckt worden. Die Daten der übrigen Mandanten des Steuerberaters seien gelöscht worden.

Die Staatsanwaltschaft hält diese Verfahrensweise für unbedenklich. Die zunächst durchgeführte Datensicherung sei zur Durchsicht der Unterlagen gem. § 110 StPO erfolgt. Die für das Strafverfahren bedeutsamen Daten seien mit den anderen Daten zunächst so verbunden gewesen, dass ohne diese Durchsicht eine Trennung nicht möglich gewesen sei. Es habe dem Verhältnismäßigkeitsgrundsatz entsprochen, bei einer Abwägung zwischen den Geheimhaltungsinteressen der Drittbetroffenen und den Bedürfnissen einer wirksamen Strafverfolgung im vorliegenden Zusammenhang unter den dargestellten Maßgaben den Strafverfolgungsinteressen das größere Gewicht beizumessen.

Eine Durchsicht wäre nach Auffassung der Staatsanwaltschaft nur dann unzulässig gewesen, wenn nicht zu erwarten gewesen wäre, dass sie beschlagnahmefähige Beweise zutage fördern könnte. Eine solche Erwartung habe jedoch bei dem hier vorliegenden Sachverhalt bestanden.

Die Staatsanwaltschaft räumt ein, dass in der Mitnahme der Datenträger zum Zweck der anschließenden Sichtung eine gegenüber der Datensichtung vor Ort zusätzliche Beschwer der betroffenen Dritten liegt. Den Rechten der Dritten sei aber ausreichend Rechnung getragen, wenn die kopierten gesichteten Daten, soweit sie nicht für das anhängige Ermittlungsverfahren relevant seien, unverzüglich gelöscht würden und nur zum Zwecke der Sichtung verwendet würden. So sei vorliegend verfahren worden.

Aus der Sicht des LfD ist dem im Ergebnis zuzustimmen: Wenn eine Datensichtung vor Ort wegen des Umfangs der in Rede stehenden Daten und wegen der Komplexität des Sachverhalts sowie der Datenspeicherungen nicht möglich erscheint bzw. für alle Beteiligten unzumutbar ist, dann ist die vorliegend gewählte Verfahrensweise unabweisbar. Durch die zeitnahe Löschung der Daten, die als für das Strafverfahren nicht erforderlich erkannt wurden, ist aus der Sicht des LfD auch dem Recht der betroffenen Dritten ausreichend Rechnung getragen worden. Eine weitere Frage, die sich in diesem Fall nicht konkret gestellt hat, ist jedoch, ob dann ein Verwertungsverbot für Strafverfolgungszwecke besteht, wenn die Staatsanwaltschaft/Steuerfahndung bei der Durchsicht Hinweise auf weitere Steuerdelikte anderer Mandanten erhält. Aus datenschutzrechtlicher Sicht dürften solche Zufallsfunde grundsätzlich nicht verwertet werden.

7.3.5 Polizeiliche Anfragen bei TK-Dienstleistern nach der Rufnummer von Anrufern

Das Ersuchen einer staatlichen Stelle an den Erbringer von Telekommunikationsdienstleistungen, ihr mitzuteilen, von welchem Telefonanschluss mit welchem Inhaber zu einer bestimmten Zeit ein Telefonat mit der ersuchenden staatlichen Stelle selbst geführt wurde, zielt auf einen Eingriff in das Telekommunikationsgeheimnis. Die angeforderten Daten werden vom Schutzbereich des Art. 10 GG erfasst (vgl. den sog. „Fangschaltungsbeschluss“ des BVerfG vom 25. März 1992; NJW 92, 1875 ff.). Auch private Telekommunikationsdiensteanbieter sind verpflichtet, dessen Schutz zu garantieren (§ 85 Abs. 2 TKG).

Ein solcher Eingriff in den Schutzbereich des Art. 10 GG darf nur erfolgen, wenn er entweder durch eine gesetzliche Vorschrift oder durch die Einwilligung der Betroffenen, wozu gerade auch der Anrufer zählt, gerechtfertigt ist.

Ein Polizeipräsidium wollte von einem privaten TK-Anbieter die Telefonnummer und die Namensangaben einer Person erfahren, die mit einem Polizeibeamten telefoniert und dabei ihre Rufnummer nicht unterdrückt hatte: Diese war im Display des angerufenen Apparats erschienen; der angerufene Polizeibeamte konnte sie sich allerdings nicht aufschreiben.

Der TK-Diensteanbieter weigerte sich, die Daten ohne richterlichen Beschluss herauszugeben. Im Unterschied zu Polizei und Staatsanwaltschaft sah er in der Unterlassung, die Rufnummernaktivierung zu unterdrücken, keine wirksame Einwilligung des Anrufers in die Übermittlung seiner Telefonnummer durch den TK-Anbieter an die von ihm angerufene Polizeidienststelle. Der LfD stimmte dem TK-Anbieter zu: In dem Verzicht auf die Aktivierung der Rufnummernunterdrückung liegt eine temporäre Bekanntgabe dieser Information an den Angerufenen. Eine Dauerwirkung entfaltende rechtlich wirksame Erklärung, der Angerufene dürfe sich diese Information mit Hilfe des TK-Anbieters zu einer beliebigen Zeit auch nach dem Telefonat noch beschaffen, kann darin nicht gesehen werden.

Als gesetzliche Ermächtigung blieben also nur die §§ 100 g, h StPO. Deren Voraussetzungen lagen im hier zu beurteilenden Fall aber nicht vor. Auch an § 34 StGB – an den Fall des übergesetzlichen Notstands – kann, im Ausnahmefall der Gefährdung höherwertiger Rechtsgüter, gedacht werden. Die Voraussetzungen dieser Norm hatten im konkreten Fall aber ebenfalls nicht vorgelegen.

Im Ergebnis hat der LfD damit die Rechtsauffassung des Netzbetreibers geteilt. Diese führt aus seiner Sicht auch keinesfalls zu praktisch untragbaren oder unhaltbaren Ergebnissen. Das Ministerium der Justiz hat mitgeteilt, dass es diese Rechtsauffassung ebenfalls unterstützt.

7.3.6 Datenerhebungen bei einer Kassenärztlichen Vereinigung durch die Polizei im Zusammenhang mit Ermittlungen wegen Kindstötung

Aufgrund einer Pressemeldung wurde der LfD darauf aufmerksam, dass die Polizei im Zusammenhang mit Ermittlungen wegen Kindstötung ärztliche Daten über junge Frauen erhoben hatte, die zu einem bestimmten Termin entbinden sollten. Folgender Sachverhalt hat sich aus den anschließenden Feststellungen ergeben:

Auf der Grundlage eines mit der Staatsanwaltschaft abgestimmten schriftlichen Ersuchens des zuständigen Polizeipräsidiums hatte der Leiter der Abrechnungsstelle der KV den ermittelnden Beamten eine Diskette mit den Datensätzen von den Frauen übergeben, die bei einem über die KV abrechnungsberechtigten Arzt in Behandlung waren und einen errechneten Geburtstermin in einem bestimmten Zeitraum hatten.

Die Polizei schied aus diesem Datenbestand die Mütter aus, deren Geburt amtlich registriert war. Die verbleibenden Frauen, bei denen keine Geburt festgestellt werden konnte, wurden schriftlich befragt. Die Befragten übermittelten entweder Bescheinigungen über Abtreibungen oder Totgeburten.

Nach Unterrichtung über diesen Vorgang wurde die fragliche Ermittlungsaktion umgehend durch den Leitenden Oberstaatsanwalt gestoppt und die bis dahin entstandenen Unterlagen, soweit sie dem Arztgeheimnis unterlagen, wurden vernichtet.

Aus datenschutzrechtlicher Sicht war zunächst festzustellen, dass die KV die verlangte Auskunft nicht hätte erteilen dürfen. Diese Daten unterliegen auch bei der KV der ärztlichen Schweigepflicht, § 76 Abs. 1 SGB X. Danach gilt, dass von einem Arzt übermittelte Daten von der KV nur unter den Voraussetzungen weiter übermittelt werden dürfen, unter denen der Arzt selbst dazu befugt gewesen wäre. Im vorliegenden Fall waren die behandelnden Ärzte an das strafbewehrte Arztgeheimnis i. S. d. § 203 Abs. 1 StGB gebunden; sie hätten nicht übermitteln dürfen, eine Befugnis dazu lag nicht vor. Die Datenübermittlung war also rechtswidrig.

Die Strafverfolgungsbehörden dürfen keine Anstiftung zu Handlungen leisten, die rechtswidrig sind. Dies ergibt sich aus allgemeinen rechtsstaatlichen Gründen, aber auch aus § 14 Abs. 1 LDSG, wonach die ersuchende Stelle grundsätzlich die Verantwortung für die Rechtmäßigkeit der Übermittlung trägt. Auch die Strafverfolgungsbehörden haben damit aus der Sicht des LfD gegen Datenschutzrecht verstoßen.

Der Leiter der zuständigen Staatsanwaltschaft teilte diese Auffassung; sie reagierte unmittelbar und veranlasste die Löschung der erhobenen Daten.

7.3.7 Unzulässige Abrufe aus einem staatsanwaltschaftlichen Verfahrensregister?

Ein Beschwerdeführer hat sich mit folgendem Vorbringen an den LfD gewandt: Sein Nachbar sei als Geschäftsstellenleiter bei einem Amtsgericht tätig. Seine Ehefrau sei Mitarbeiterin der örtlichen Staatsanwaltschaft. Der Nachbar habe ihn – seiner Auffassung nach zu Unrecht – in einer Anzeige beschuldigt, zwei Thuja-Bäume um etwa 50 bis 60 cm abgeschnitten zu haben, ohne dazu berechtigt zu sein. Er habe bereits in der Strafanzeige bei der Rechtsantragstelle der Staatsanwaltschaft zu Protokoll gegeben, dass ihm bekannt sei, dass gegen den Beschuldigten schon mehrere Verfahren wegen vergleichbarer Delikte anhängig gewesen seien. Diese seien jedoch jeweils eingestellt worden.

Der Beschwerdeführer hat die Frage gestellt, wie sein Nachbar überhaupt über die vorgeschilderten Strafverfahren informiert sein konnte. In einer Stellungnahme hat der Geschäftsstellenleiter erklärt, dass er die in Rede stehende Information „von privaten Leuten erzählt bekommen“ habe. Der Verdacht war sicher nicht fern liegend, dass Informationsquelle dafür seine Ehefrau sein könnte, die möglicherweise Zugriff auf staatsanwaltschaftliche Informationssysteme sowie staatsanwaltschaftliche Akten hatte.

Die Nutzung dienstlich erlangter Kenntnisse zu privaten Zwecken ist aus der Sicht des LfD zumindest datenschutzrechtlich unzulässig. Deshalb hat er den behördlichen Datenschutzbeauftragten der Staatsanwaltschaft gebeten, der Sache nachzugehen und ihn über das Ergebnis seiner Überprüfung zu unterrichten. Dieser hat Folgendes mitgeteilt:

Die Ehefrau des Anzeigeerstatters sei aufgrund ihres Tätigkeitsfeldes berechtigt, auf die im staatsanwaltschaftlichen Informationssystem gespeicherten Daten zuzugreifen. Es erfolge allerdings keine Protokollierung darüber, welche Person welche Daten zu welchem Zeitpunkt aufgerufen und zur Kenntnis genommen hat. Anhand des automatisierten Systems konnte also nicht überprüft werden, ob sie die betreffenden Datensätze aufgerufen hat. Eine persönliche Befragung der Mitarbeiterin durch den genannten behördlichen Datenschutzbeauftragten der Staatsanwaltschaft hat keine weiteren Erkenntnisse ergeben. Sie hat angegeben, sie habe zu keinem Zeitpunkt auf Daten des Beschwerdeführers zugegriffen.

Die Möglichkeiten zur Aufklärung der Angelegenheit waren damit ausgeschöpft. Der Fall verdeutlicht, dass die Protokollierung von Datenzugriffen wichtig ist und auch zur Entlastung von verdächtigten Mitarbeitern öffentlicher Stellen beitragen könnte.

7.3.8 Archivierung von Strafverfahrensakten mit ärztlichen Unterlagen

Fraglich war, ob eine Abgabe von Strafverfahrensakten mit höchst sensiblen ärztlichen Unterlagen an das Staatsarchiv mit dem Grundrecht auf Datenschutz der betroffenen Zeuginnen vereinbar war. Der LfD hat eine entsprechende Anfrage des Ministeriums der Justiz wie folgt beantwortet:

– Die in den Strafverfahrensakten vorhandenen Zeugenaussagen unterliegen auch dann, wenn sie den Gesundheitsbereich betreffen, keiner besonderen Geheimhaltungspflicht, die dem Arztgeheimnis entsprechen würde. Allerdings gilt für diese Unterlagen das Amtsgeheimnis, das von §§ 203 Abs. 2, 353 b StGB geschützt ist. Außerdem ist der Grundgedanke von Art. 8 der EG-Datenschutzrichtlinie bei der Auslegung der nationalen Gesetze zu beachten, auch wenn diese Regelung über den besonderen Schutz von Gesundheitsdaten im Bereich der Strafverfolgung nicht unmittelbar anwendbar ist. Jedenfalls begründet die Sensitivität dieser Informationen eine besondere Pflicht zur strikten Beachtung der datenschutzrechtlich relevanten Vorgaben der Strafprozessordnung und untergesetzlicher Vorschriften (beispielsweise auch der Aufbewahrungsbestimmungen).

– Auch soweit beschlagnahmte ärztliche Unterlagen Bestandteil der Strafverfahrensakten geworden sind, gilt für diese das Arztgeheimnis nicht mehr unmittelbar: Eine Erstreckung des Arztgeheimnisses auf Stellen, die ärztliche Unterlagen rechtmäßigerweise erhalten haben, ist gesetzlich nicht geregelt. Hierfür gilt also im Ergebnis das Gleiche wie zu den oben erwähnten Unterlagen.

– Die Regelungen des Landesarchivgesetzes, wonach für amtliche Unterlagen eine Anbietungspflicht gegenüber dem zuständigen Staatsarchiv besteht, gelten sogar für solche Informationen, die einer besonderen Geheimhaltungspflicht unterworfen sind. Aus Sicht des LfD zitiert die Generalstaatsanwaltschaft Koblenz im vorliegenden Zusammenhang zutreffenderweise § 7 Abs. 2 LArchG. Die vorliegend in Rede stehenden Akten unterliegen also ebenfalls dieser Pflicht. Der Gesetzgeber hat in einer verfassungsrechtlich nicht zu beanstandenden Weise im Landesarchivgesetz geregelt, dass das „kollektive Gedächnis“ der Gesellschaft für künftige Generationen (als das die Archive anzusehen sind) auch solche Unterlagen umfassen soll, die besonders schutzbedürftig und in besonderer Weise dem gegenwärtigen Zugriff Dritter entzogen sind.

– Der Wahrung der datenschutzrechtlichen Belange dienen in diesem Zusammenhang besonders zwei Mechanismen:

  Zum einen dürfen die Staatsarchive nur solche angebotenen Unterlagen übernehmen, die nach ihren eigenen generellen Kriterien als archivwürdig anzusehen sind. Dies bedeutet, dass unabhängig von der Sensibilität der Daten nach archivfachlichen Kriterien eine Auswahl zu erfolgen hat; nur ein relativ kleiner Teil der angebotenen Datenbestände wird in das Archiv übernommen. Es ist keinesfalls vorgesehen, dass vollständige behördliche Datenbestände zum Archivbestandteil werden. Die die Auswahl treffenden zuständigen Archivare unterliegen sowohl dem Amtsgeheimnis (das strafbewehrt ist) wie den Anforderungen des Datenschutzrechts.
  Zum anderen gelten im Staatsarchiv für die Nutzung von solchen Unterlagen, die schutzbedürftig sind, ausreichend lange Schutzfristen. So dürfen entsprechende Unterlagen frühestens 30 Jahre nach dem Tod der Betroffenen genutzt werden (§ 3 Abs. 3 Satz 1 LArchG). Außerdem hat das Staatsarchiv selbst in den Fällen der grundsätzlich zulässigen Nutzung die Pflicht zu prüfen, ob nicht besondere Auflagen bei der Nutzung solcher Unterlagen geboten sind (§ 3 Abs. 2 LArchG). Für Unterlagen der hier in Rede stehenden Art wäre aus datenschutzrechtlicher Sicht sogar (im Sinne eines „Zwei-Schranken-Prinzips“) eine analoge Anwendung der Schutzfrist von 80 Jahren nach Entstehung angemessen, die für Daten gilt, die einer besonderen gesetzlichen Geheimhaltungspflicht unterliegen (§ 3 Abs. 3 Satz 2 LArchG).

Vor diesem Hintergrund hat sich der LfD bei Erlass des Landesarchivgesetzes diesen Regelungen nicht entgegengestellt und damit akzeptiert, dass auch besonders sensible und besonders schutzbedürftige Akten dem Staatsarchiv angeboten und – in einem beschränkten Umfang – dort archiviert werden dürfen.

7.4 Strafvollzug

7.4.1 Allgemeines zu den Eingaben Strafgefangener

Es gab einige erfolgreiche Eingaben Strafgefangener, die im Allgemeinen aber auf eher weniger gravierende Fehler der Justizvollzugsanstalten hinwiesen. Diese betrafen etwa folgende Punkte:

– Besucherinformation entgegen dem ausdrücklichen Wunsch des Gefangenen
– Verweigerung des Einsichtsrechts in Personalakten
– Übersendung des A-Bogens an das unzuständige Verwaltungsgericht
– Personenverwechslung bei der Aushändigung von Schreiben
– Nichtlöschung einer getilgten Strafe in der Personalakte
– Verbesserung des Bescheid-Versandes durch Strafvollstreckungsgerichte
– Verbesserung des Verfahrens beim Erstellen von Kopien für Gefangene.

Nicht selten musste bzw. konnte der LfD Eingaben schon ohne Beteiligung der JVA bzw. des Ministeriums der Justiz den beschwerdeführenden Strafgefangenen abschlägig bescheiden, weil erkennbar kein Datenschutzverstoß vorliegen konnte. Dies erfolgte auch, um die Arbeitsbelastung der Vollzugsanstalten so gering wie möglich zu halten. Dabei waren z. B. folgende Themen angesprochen worden:

– Die offene Weiterleitung von Schreiben des Ministeriums der Justiz über die JVA an den Beschwerdeführer.
– Die Frage, ob ein Strafgefangener einen Anspruch auf Fertigung und Aushändigung von Personalausweiskopien hat.

Etwa ein Fünftel der Eingaben (drei bis vier pro Jahr) dürfte im Ergebnis für die Petenten erfolgreich sein.

Der Strafvollzug bildet durchaus keinen Schwerpunkt der Tätigkeiten des LfD, die JVAs und die Strafvollzugsabteilung des Ministeriums der Justiz werden mit dessen Prüfmaßnahmen (insbesondere Aufforderungen zur Stellungnahme) aus der Sicht des LfD nicht unangemessen belastet.

7.4.2 Antrag auf Einsicht in Gefangenenpersonalakten und auf Überlassung von Fotokopien daraus

Ein Gefangener hat sein Anliegen auf Akteneinsicht, das die JVA abgelehnt hatte, dem LfD gegenüber wie folgt näher begründet:

Er erstrebe eine „tatsachengerechte Vollzugsplanung“. Er meinte, die psychologischen Gutachten enthielten „rechtswidrige Erkenntnisse“. Vermerke seien tatsachenwidrig. In Stellungnahmen der psychologischen Mitarbeiter der JVA seien pflichtwidrige Unterlassungen festzustellen. Gegen bestimmte Behauptungen wolle er sich gerichtlich wehren. Die Einsichtnahme sei in der Form der Überlassung von Kopien zu gewähren. Grund dafür sei, dass die jeweiligen Unterlagen sehr umfangreich seien. So umfasse allein das Gutachten eines bestimmten Psychiaters ca. 70 Seiten.

Letztlich rügte der Gefangene eine unzutreffende Wertung seiner Persönlichkeit und seiner Aktivitäten durch die Psychologen der Anstalt und durch externe Sachverständige.

Es besteht zwar kein rechtlich durchsetzbarer Anspruch auf eine bestimmte psychologische Wertung durch sachverständige Personen. Das Anliegen, auf der Basis zutreffender Sachverhalte psychologisch beurteilt zu werden, ist jedoch aus Sicht des LfD als rechtliches Interesse anzuerkennen. Die vom Gefangenen erhobene Rüge „pflichtwidriger Unterlassungen" ist allerdings sehr unbestimmt, so dass nicht beurteilt werden kann, ob sich auch unter diesem Gesichtspunkt ein entsprechendes rechtliches Interesse ergeben kann.

Um genau benennen zu können, welche Tatsachenbehauptungen der Gutachter aus seiner Sicht falsch sind und um dazu ggf. gerichtliche Hilfe in Anspruch nehmen zu können, ist der Gefangene auf die genaue Kenntnis der in Frage kommenden Gutachten – nicht nur auf die Mitteilung der darin enthaltenen Wertungen und Schlussfolgerungen – angewiesen. Insoweit ist also nach Auffassung des LfD ein Anspruch auf Akteneinsichtnahme grundsätzlich anzuerkennen.

Die wesentlichen Gesichtspunkte, die aus der Sicht der JVA begründen, dem Gefangenen eine bestimmte weitere Berufsausbildung nicht zu ermöglichen und die es weiterhin begründen, von einer fehlenden Mitarbeit am Vollzugsziel auszugehen, sind ihm zwar mitgeteilt worden. Dem Gefangenen muss aber ermöglicht werden, unter den o. g. Gesichtspunkten die Richtigkeit der diesen Wertungen zugrunde liegenden Gutachten und der darin enthaltenen tatsächlichen Feststellungen zunächst selbst zu überprüfen und dann dies auch ggf. gerichtlich zu veranlassen. Daraus folgt, dass er Gelegenheit erhalten muss, zur (ggf. auch gerichtlichen) Geltendmachung bestimmter Ansprüche gegenüber der JVA in bestimmte Gutachten, die die Wertungen der JVA bezüglich seiner Behandlung wesentlich bestimmen, Einsicht zu nehmen.

Zum Recht auf Fertigung von Abschriften bzw. von Kopien der psychologischen Basisdiagnostik hat die Strafvollstreckungskammer Diez des LG Koblenz mit Beschluss vom 16. Mai 2002, Az. 7 StVK 956/00, auf der Grundlage einer Entscheidung des OLG Koblenz vom 5. Juli 2001 Folgendes entschieden:

Ein rechtliches Interesse des Gefangenen bestehe an der Akteneinsicht (wobei die Fertigung von Abschriften/Kopien Formen der Akteneinsicht seien), wenn „die Auskunftserteilung zur Wahrung seiner Interessen nicht ausreiche". Die psychologische Basisdiagnostik sei für einen Strafgefangenen von ganz erheblicher Bedeutung. Sie bilde eine der Grundlagen für die Erreichung des Vollzugsziels gem. § 2 Abs. 1 StVollzG.

Vor diesem Hintergrund hält es der LfD insbesondere dann, wenn es sich um komplexe schriftliche Ausführungen handelt, für geboten, dem Gefangenen Kopien derjenigen Unterlagen und Gutachten des psychologischen Dienstes der JVA zu gewähren, die als unmittelbare Grundlage der Entscheidungen der JVA für die Vollzugsplanung dienen. Insoweit sollte die JVA aus datenschutzrechtlicher Sicht die Anträge des Gefangenen im Sinne einer seinen Interessen gerecht werdenden Fürsorge auslegen und ihn entsprechend bescheiden. Eine zu engherzige Auslegung des Auskunfts- und Akteneinsichtsanspruches läge – jedenfalls aus der Perspektive des Grundrechtsschutzes – nicht im überwiegenden Allgemeininteresse.

Leider ist es dem LfD nicht gelungen, hier zu einer Übereinstimmung mit dem Ministerium der Justiz zu kommen.

7.4.3 Fertigung von Lichtbildern bei Strafgefangenen, insbesondere Vernichtung bei Entlassung

Die Frage der erkennungsdienstlichen Behandlung von Strafgefangenen, insbesondere die Fertigung von Lichtbildern, ist in § 86 Abs. 3 StVollzG geregelt.

In der Praxis wird wohl in nahezu allen Bundesländern (von wenigen Ausnahmen abgesehen) folgendermaßen verfahren:

Bei der Aufnahme von Strafgefangenen in die JVA wird unabhängig von der Dauer der Strafhaft ein Lichtbild gefertigt und zur Gefangenenpersonalakte genommen. Lichtbilder werden in verschiedenen Zusammenhängen in der JVA genutzt (zur Fertigung von Hausausweisen, zur Nutzung durch die Pforte etc.). Dabei verfährt die Praxis anders, als es der Gesetzeswortlaut nahe legt („zur Sicherung des Vollzuges sind zulässig ... die Aufnahme von Lichtbildern ..."): Es werden in jedem Fall ohne Ermessensausübung und ohne Einzelfallprüfung Lichtbilder gefertigt.

Es wird seitens der Justiz vorgetragen, man könne zu Beginn des Vollzuges unabhängig von der Dauer der Strafhaft eine Fluchtgefahr so gut wie nie ausschließen, selbst wenn sich der Strafgefangene freiwillig zum Strafantritt gemeldet habe. Außerdem diene das Lichtbild nicht nur im Falle der Flucht zur Unterstützung der Fahndung. Es diene auch innerhalb der JVA der Verhinderung von Verwechslungen. Gerade auch bei Freigängern diene es schließlich der Prävention bezüglich der Begehung weiterer Straftaten und der Flucht. Soweit die Vollzugsgeschäftsordnung in Nr. 23 Abs. 2 eine Beschränkung enthält, wonach erst von Strafgefangenen mit einer Vollzugsdauer von einem Jahr und mehr sowie von Sicherungsverwahrten Lichtbilder aufzunehmen seien, wird erklärt, diese Vorgabe werde als obsolet angesehen. Es bestünden einvernehmliche Bestrebungen, die Vollzugsgeschäftsordnung insoweit zu ändern. Den JVAs sei freigestellt, sich daran nicht mehr zu halten.

Nun hat der LfD durchaus Verständnis für die Auffassung der Vollzugsseite, nicht in jedem Einzelfall eine zu begründende Ermessensentscheidung über die Fertigung von Lichtbildern zu treffen, sondern in jedem Fall routinemäßig solche Bilder anzufertigen. Für unverhältnismäßig und aus datenschutzrechtlicher Sicht nicht hinnehmbar hält er allerdings, dass einmal gefertigte Licht-

bilder gemäß der neuen Regelung des § 86 Abs. 3 StVollzG auch weit über die Dauer der Strafhaft hinaus als Bestandteil der Gefangenenpersonalakten aufbewahrt werden, nachdem dort ausdrücklich geregelt ist, dass Lichtbilder nicht wie sonstige erkennungsdienstliche Unterlagen bei der Entlassung zu vernichten sind, sondern dass diese als Teil der Gefangenenpersonalakte deren Schicksal teilen.

Es gäbe zwei Möglichkeiten zur Änderung dieser unbefriedigenden Situation:

1. § 86 Abs. 3 StVollzG wird verfassungskonform so ausgelegt, dass jedenfalls im Zeitpunkt der Entlassung eine Ermessensentscheidung über die weitere Aufbewahrung der Lichtbilder erfolgt und nur in Ausnahmefällen die Lichtbilder aufbewahrt werden.
2. Der Wortlaut der Regelung wird geändert, so dass dort bezüglich der Vernichtung von Lichtbildern nach Entlassung ausdrücklich eine Ermessensentscheidung gefordert wird.

Andernfalls sind Fälle wie der nachfolgend geschilderte an der Tagesordnung: Wegen Verstoßes gegen das Pressegesetz musste ein Betroffener eine Strafhaft von sieben Monaten verbüßen. Er stellte sich freiwillig zum Strafantritt. Dennoch wurde ein Lichtbild gefertigt, dessen Vernichtung er nach Abschluss der Strafhaft nicht erreichen konnte. Die Strafvollstreckungskammer wies mit bloßem Hinweis auf § 86 Abs. 3 StVollzG seinen entsprechenden Antrag zurück.

Die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder, eine Gesetzesänderung zu erreichen, waren erfolglos. Auch ihr Anliegen, auf der Ebene der Verwaltungsvorschriften (in Nr. 23 der Vollzugsgeschäftsordnung) die Pflicht zur Ermessensentscheidung über den weiteren Verbleib des Lichtbilds in der Akte nach Entlassung des Strafgefangenen zu erreichen, wurde nicht verwirklicht.

7.4.4 Offene Aushändigung von Kontoauszügen an Strafgefangene

Mehrere Strafgefangene haben sich an den LfD gewandt und gerügt, dass ihnen die Mitteilung über ihre finanziellen Verhältnisse (Geldbewegungen auf ihren verschiedenen Konten der Anstalt) von Bediensteten offen übergeben würden. Dies verstoße gegen den Datenschutz, da diese Mitarbeiter des Justizvollzuges ihr Guthaben nichts anginge.

Zu diesem Thema gibt es auf der Ebene der Strafvollstreckungskammern unterschiedliche Rechtsprechung; so hat die Strafvollstreckungskammer Trier – ebenso wie die Strafvollstreckungskammer Karlsruhe, aber abweichend von der des LG Koblenz – diesen Anspruch der Strafgefangenen anerkannt.

Das OLG Koblenz hat (mit Beschluss vom 21. Juli 2003, Az. 1 Ws 303/03) im Ergebnis das datenschutzrechtliche Anliegen, Kontoauszüge den Gefangenen nur in verschlossenen Umschlägen auszuhändigen, zurückgewiesen. Es hat sich insoweit einem Beschluss des OLG Hamburg (vom 7. April 2003, Az. 3 Vollz (Ws) 31/03) angeschlossen.

Der LfD hat in diesem Zusammenhang gegenüber dem Justizministerium folgende Gesichtspunkte betont, die auch das Oberlandesgericht hervorgehoben hat:

1. Bei den Daten auf den in Rede stehenden Kontoauszügen handelt es sich um schützenswerte personenbezogene Daten der Gefangenen.
2. Es gibt keine Erforderlichkeit, die entsprechenden Informationen allen Justizvollzugsbediensteten zur Verfügung zu stellen, die mit den Strafgefangenen in Kontakt kommen.
3. Die Frage, ob zum Schutz der hier in Rede stehenden personenbezogenen Daten verschlossene Umschläge einzusetzen sind, ist allein danach zu beurteilen, ob es sich hierbei um eine vom Aufwand her angemessene Maßnahme im Sinne des Datenschutzes handelt (§ 183 StVollzG i. V. m. § 9 BDSG).
4. Bei dieser Beurteilung ist das Oberlandesgericht zum Ergebnis gekommen, dass der hier zu treibende Aufwand letztlich nicht in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stünde.

Vor dem Hintergrund der oben unter 1. und 2. wiedergegebenen Grundsätze ist aus der Sicht des LfD seitens der JVAs allerdings darauf zu achten, dass – auch unterhalb der Schwelle des Einsatzes verschlossener Umschläge – die hierzu eingesetzten Bediensteten beim Austeilen von den entsprechenden Kontoauszügen und sonstigen Unterlagen grundsätzlich keine Kenntnis nehmen und ausnahmsweise dennoch erlangte Kenntnisse nicht missbräuchlich verwenden. Die JVAs sollten ihre Bediensteten entsprechend verpflichten. Der LfD hat das Justizministerium auf diese Auffassung hingewiesen.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 Datenschutz in der Schule

Das Ministerium für Bildung, Frauen und Jugend hat im April 2003 eine neue Bekanntmachung zu „Datenschutz und Datensicherheit in Schulen bei der Verarbeitung personenbezogener Daten in automatisierten Verfahren oder in Akten“ herausgegeben und damit die Bekanntmachung von 1996 überarbeitet. Dass das Thema Datenschutz in der Schule in den letzten Jahren an Bedeutung gewonnen hat, ist nicht nur dem wesentlich gewachsenen Umfang dieser Veröffentlichung zu entnehmen. In dem Werk finden insbesondere Lehrerinnen und Lehrer Antwort auf viele datenschutzrechtliche Fragen.

8.1.2 Mehr Rechte für Eltern – Einschränkung des informationellen Selbstbestimmungsrechts von Schülern

Nach dem Amoklauf eines Schülers an einer Erfurter Schule im Frühjahr 2002 wurde ein Auskunfts- und Informationsrecht der Eltern volljähriger Schüler diskutiert. Einige Länder planten, ihre Schulgesetze zu ändern und die Recht der Eltern zu erweitern, insbesondere eine Informationspflicht einzuführen. Eine entsprechende Gesetzesänderung erfolgte auch in Rheinland-Pfalz. Bisher hatten die Eltern volljähriger Schüler lediglich das Recht, sich über deren Ausbildungsweg zu unterrichten. Im Mittelpunkt der neuen Regelung stand die Pflicht der Schulen, die Eltern volljähriger Schüler über bestimmte aufgeführte Ereignisse zu informieren. Die Schulen hätten nach einem ersten Änderungsentwurf ohne jeglichen pädagogischen Spielraum bei Vorliegen der Voraussetzungen die Eltern einschalten müssen.

Gegenüber dem Ministerium für Bildung, Frauen und Jugend hatte der LfD Zweifel an der Geeignetheit dieser Maßnahmen zum Ausdruck gebracht. Er regte an, die Einschaltung von Schulpsychologen und Vertrauenslehrern zu erwägen und die Tatsache zu berücksichtigen, dass nicht alle volljährigen Schüler ausreichend Kontakt zu ihren Eltern haben. Geeignet erschien eine Unterrichtung der Eltern nur, wenn diese ins Ermessen der Schule gestellt würde, die dann aufgrund ihrer eigenen Erfahrungen und Kenntnisse der familiären Verhältnisse des Schülers entscheiden kann, ob eine Einbeziehung der Eltern Erfolg versprechend erscheint.

Diese Bedenken wurden vom Ministerium aufgegriffen. Auf die ausdrückliche Informationspflicht wurde zugunsten einer Sollvorschrift verzichtet. Dies bedeutet, dass die Schule in Ausnahmefällen die Möglichkeit hat, von einer Information der Eltern abzusehen.

8.1.3 Einwilligungsfähigkeit von Minderjährigen

Aus den Schulen wurde im Zusammenhang mit der Veröffentlichung von personenbezogenen Daten im Internet immer wieder die Frage an den LfD herangetragen, inwieweit Minderjährige wirksam einwilligen können.

Die datenschutzrelevante Einwilligungsfähigkeit ist nicht an die Volljährigkeit geknüpft. Schüler sind dann allein einwilligungsfähig, wenn sie die Bedeutung und Tragweite der Einwilligung und ihrer rechtlichen Folgen erfassen können und ihren Willen hiernach zu bestimmen vermögen. Ob dies für einen Schüler zutrifft, ist letztlich nur unter Abwägung der konkreten Datenübermittlung und der Kenntnis der Persönlichkeit des einzelnen Schülers zu entscheiden. Dies wird jedoch in der Praxis nicht mit verhältnismäßigen Mitteln durchzuführen sein. Der LfD hat daher empfohlen, eine feste Alters- oder Klassengrenze zu bestimmen, ab der es nur noch auf die Einwilligung der Schüler ankommt. Dies könnte ab der 10. Klasse oder der Oberstufe gelten, da in diesem Alter die Schüler wohl allgemein über die entsprechende Einsichtsfähigkeit bezüglich der Veröffentlichung ihrer Daten im Internet verfügen.

8.1.4 Videoüberwachung in der Schule

Eine Schule beabsichtigte, einen Raum für Schüler einzurichten, in dem diese still arbeiten konnten. Da eine Beaufsichtigung durch Lehrer nicht möglich war, war an eine Überwachung mittels Videokamera gedacht.

Die Installation einer solchen Videokamera stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Schüler dar. Ein solcher Eingriff ist nur unter engen Voraussetzungen zulässig.

Das am 8. Mai 2002 neu in Kraft getretene LDSG enthält in § 34 eine Regelung zur Videoüberwachung öffentlich zugänglicher Räume. Auch wenn der Schülerarbeitsraum nicht öffentlich zugänglich war, empfahl der LfD, die dort genannten Vorgaben entsprechend umzusetzen. Danach ist die Videoüberwachung nur zulässig, soweit dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Im vorliegenden Fall war fraglich, ob die Installation einer Videoüberwachung als erforderlich beurteilt werden konnte. Mit der Installation sollte eine ordnungsgemäße Nutzung des Arbeitsraumes sichergestellt werden. Unter ordnungsgemäßer Nutzung war hier das Aufsuchen des Raumes von Schülern in der unterrichtsfreien Zeit zu verstehen, um mit den dort vorhandenen Hilfsmitteln schulische Aufgaben zu erledigen (z. B. Hausaufgaben, Referate etc.). Der Raum sollte erst eingerichtet werden. Dies bedeutete, dass die Schule noch keinerlei Erfahrung gemacht hatte, ob es zu Störungen durch Schüler kommt. Aus datenschutzrechtlicher Sicht gab es daher weit weniger eingriffsintensive Maßnahmen, um einen ordnungsgemäßen Gebrauch sicherzustellen. Der LfD

empfahl den Erlass einer Nutzungsordnung, zu deren Einhaltung sich alle Schüler verpflichten sollten, die den Arbeitsraum aufsuchen wollten. Erst wenn es dennoch zu Störungen kommen würde, wäre eine Videoüberwachung zur Aufrechterhaltung des Hausrechts als erforderlich anzusehen. In diesem Fall wären die weiteren Bedingungen für eine Videoüberwachung nach LDSG einzuhalten. Insbesondere wäre die Videoüberwachung erkennbar zu machen.

8.1.5 Einsatz von Sniffer-Programmen zur Überwachung der PC-Netzwerke

Dem LfD wurde durch den Redakteur einer Schülerzeitung zugetragen, dass an dessen Schule ein sog. Sniffer-Programm auf einem für Schüler und Lehrer frei zugänglichen PC installiert wurde. Dieses Programm ist in der Lage, jede Tastaturfunktion zu protokollieren. Dadurch wird also nicht nur der Benutzer des PCs erfasst, sondern z. B. auch ein gesamtes Textdokument, das dieser erstellt hat. Die Protokolldaten können an jede beliebige Emailadresse versandt werden. Für den Benutzer ist es nicht erkennbar, dass seine Eingaben detailliert protokolliert werden. Auch ist das Programm auf dem Rechner nur schwer auffindbar. Im vorliegenden Fall hatte wahrscheinlich ein Schüler, der den Rechner im Auftrag der Schule betreute, dieses Programm ohne Wissen der Schulleitung installiert und sich die Protokolle an seine Emailadresse schicken lassen. Nachdem die Angelegenheit bekannt wurde, wurde das Programm sofort gelöscht und der Schüler von seiner Aufgabe entbunden.

Auch wenn ein Schüler ohne Wissen der Schulleitung ein solches Programm installiert hatte, war die Schule als datenverarbeitende Stelle anzusehen. Diese darf nach dem Schulgesetz aber nur dann personenbezogene Daten von Schülern und Lehrern erheben, wenn dies zur Erfüllung einer ihr durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgabe erforderlich ist. Auch unter dem Aspekt, dass gewisse Kontrollen der Benutzer des PCs zulässig wären, war eine detailgenaue Protokollierung der Eingaben unzulässig. Der Einsatz derartiger Programme kann auch in strafrechtlicher Hinsicht erheblich sein.

8.1.6 Meldeblatt für Schulabgänger

In einer Integrierten Gesamtschule wurde den Schülern ein Formular ausgegeben, in dem sie Name, Geschlecht, Geburtsdatum und -ort, Konfession, Staatsangehörigkeit, Adresse, Name und Anschrift der Erziehungsberechtigten, Informationen über den bisherigen Schulbesuch sowie über die Berufsabsichten angeben sollten. Das Verfahren diente der Erfassung der Entlassschüler an der berufsbildenden Schule, stellte aber keine Anmeldung zum Schulbesuch dar. Fraglich war, ob die Erhebung wirklich aller gewünschten Informationen zulässig war.

Dies beurteilte sich nach dem Schulgesetz: Danach dürfen personenbezogene Daten der Schüler durch Schulen erhoben werden, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist. Die hier erhobenen Daten sollten der Überwachung der Schulpflicht dienen, einer der Schule obliegenden Aufgabe. Die Voraussetzungen für das Bestehen der Schulpflicht und die Befreiungstatbestände sind in der Berufsschulverordnung geregelt. Für eine entsprechende Überprüfung waren aus Sicht des LfD Name, Anschrift und Geburtsdatum des Schülers sowie die Informationen über den bisherigen Schulbesuch und die Berufsabsichten erforderlich. Die Betroffenen waren insoweit zur Angabe verpflichtet. Die übrigen Erhebungen des Meldeblattes (Geschlecht, Geburtsort, Staatsangehörigkeit und Konfession) dienten nicht der Überprüfung der Schulpflicht, sondern waren erst erforderlich, wenn der betroffene Schüler tatsächlich in die Schule aufgenommen werden sollte. Die Meldung der Schulabgänger war, wie ausdrücklich vermerkt, kein Aufnahmeantrag. Daher war auf die Erhebung dieser Daten zu verzichten. Das Meldeblatt wurde inzwischen den datenschutzrechtlichen Vorgaben angepasst.

8.1.7 Übermittlung von Schulabgängerdaten an das Jugendamt

Im Rahmen eines Modellprojekts zur integrierten Stadtteil- und Jugendarbeit hatte sich eine Arbeitsgruppe „Jugendliche nach Schulabgang“ gebildet. An ihr waren u. a. das Arbeitsamt (Berufsberatung), eine Haupt- und Grundschule sowie das Jugendamt beteiligt. Ziel war es, den Schülerinnen und Schülern nach Verlassen der Schule die eventuell erforderlichen Förder- und Beratungsangebote gezielter als bisher zu vermitteln. Es hatte sich herausgestellt, dass einige Jugendliche, die nach Schulabgang keine Ausbildungsstelle finden, überhaupt keine Beratungsangebote aufsuchten. Die aufsuchende Jugendarbeit hatte in solchen Fällen sehr hilfreich intervenieren können. Die bisher zufällig entstandenen Kontakte mit den Jugendlichen sollten systematischer aufgebaut werden. Hierzu hielt man es für erforderlich, dass die beteiligte Schule die aufsuchende Jugendarbeit des Jugendamtes frühzeitig über personenbezogene Merkmale informierte, die darauf hinwiesen, dass ein Schüler nach Schulabgang möglicherweise Hilfe zum Einstieg in die Berufsausbildung benötigte. Nach Kontaktaufnahme mit den betreffenden Jugendlichen sollten alle weiteren Kontakte zu beratenden oder helfenden Einrichtungen im Einverständnis mit den Jugendlichen erfolgen. Es stellte sich die Frage, ob eine Datenübermittlung durch die Schule an das Jugendamt zulässig war.

Die Übermittlung personenbezogener Daten durch die Schule an andere öffentliche Stellen ist nach dem SchulG zulässig, soweit der Empfänger aufgrund einer Rechtsvorschrift berechtigt ist, die Daten zu erhalten, und die Kenntnis der Daten zur Erfüllung der dem Empfänger obliegenden Aufgaben erforderlich ist. Eine Übermittlungsbefugnis konnte sich aus den Vorschriften des SGB VIII ergeben. Dort ist zwar vorgesehen, dass die Jugendhilfe Sozialdaten bei den Betroffenen erhebt. Doch in Ausnahmefällen ist eine Erhebung ohne Mitwirkung der Betroffenen zulässig. Eine solche kommt u. a. dann in Betracht, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür vorliegen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Hier war zunächst die Möglichkeit in Betracht zu ziehen, dass die Schule bestimmte Schulabgänger auf die Möglichkeiten der Jugendhilfe hinwies und die Jugendlichen sodann Kontakt mit dieser aufnehmen konnten.

Damit wäre durch die Kontaktaufnahme seitens der Jugendlichen eine Datenerhebung bei den Betroffenen gewährleistet gewesen. Jedoch wurde dieses Verfahren der Arbeit der aufsuchenden Jugendarbeit nicht gerecht. Diese nahm in der Regel keinen schriftlichen Kontakt mit den Jugendlichen auf, sondern suchte das persönliche Gespräch und erkundigte sich auch bei anderen nach dem Verbleib der zu beratenden Jugendlichen. Eine Datenerhebung beim Betroffenen wäre also für die aufsuchende Jugendarbeit ein unverhältnismäßiger Aufwand gewesen, der nicht zum gewünschten Ergebnis geführt hätte. Den schutzwürdigen Belangen der Betroffenen konnte dadurch Rechnung getragen werden, dass die Schule die in Frage kommenden Jugendlichen über die beabsichtigte Datenübermittlung – Name und Anschrift – an die Jugendhilfe informierte und die Möglichkeit des Widerspruchs einräumte. Erfolgte ein solcher Widerspruch, wurde von der Datenweitergabe abgesehen. Auch das Ministerium für Bildung, Frauen und Jugend hat diese Vorgehensweise unterstützt.

8.1.8 Schülerfotografien

Immer wieder kommt es zu Unstimmigkeiten insbesondere zwischen Schule und Eltern, unter welchen Voraussetzungen Fotografien von Schülerinnen und Schülern in der Regel durch private Firmen angefertigt werden können. An der Beurteilung der datenschutzrechtlichen Voraussetzungen hat sich seit der Darstellung im 16. Tb. Tz. 8.1.5 nichts geändert. Nach wie vor gilt:

– Für die Anfertigung von Klassenfotos reicht es aus, die Klassenelternversammlung oder die Eltern in Form eines Rundschreibens über die beabsichtigten Maßnahmen zu informieren. Wer nicht möchte, dass sein Kind fotografiert wird, wird es von der Aktion fern halten oder den Lehrer entsprechend informieren.

– Sollen hingegen Einzelfotos erstellt werden, bedarf es der vorherigen ausdrücklichen Einwilligung der Betroffenen, also der Eltern und Schüler.

Die ADD hat nach dem Hinweis des LfD, dass entsprechende Fragen immer wieder an ihn herangetragen werden, die Schulen in einem Rundschreiben über die datenschutzrechtlichen Anforderungen informiert.

8.2 Hochschulen

8.2.1 Studienverlaufsstatistik

Im Rahmen der Novellierung des Hochschulstatistikgesetzes Anfang der 90ger Jahre wurde das Erhebungsverfahren umgestellt und auf eine personenbezogene Zusammenführung der Studentendaten verzichtet. Ebenso fielen die in der Vergangenheit zugelassene verwaltungsinterne Verwendungsmöglichkeit der personenbezogenen Daten und die Abiturientenbefragung weg. Gleichzeitig wurde jedoch auch der Erhebungskatalog erweitert. Dies war seinerzeit aus datenschutzrechtlicher Sicht hinnehmbar, da gleichzeitig auf die Studienverlaufsstatistik verzichtet wurde (vgl. 12. Tb. Tz. 18.3).

Nunmehr bestehen Überlegungen, die Studienverlaufsstatistik wieder einzuführen. Dies ist nach wie vor kritisch zu betrachten. Eine solche Statistik wäre nur aufgrund eines Gesetzes zulässig, das ein überwiegendes Allgemeininteresse an ihr begründet. Dabei wäre die Bildung einer zentralen Datei in personenbezogener oder –beziehbarer Form dann unverhältnismäßig, wenn die Datensätze z. B. asymmetrisch verschlüsselt werden könnten. Denn es besteht kein Interesse daran, die Person des Studierenden zu identifizieren. Es soll vielmehr möglich sein, verschiedene Datensätze ein und derselben Person zuzuordnen. Daher würde das Vorhalten verschlüsselter Datensätze bei einer zentralen Stelle ausreichen, um den angestrebten Statistikzweck zu erfüllen.

8.2.2 Evaluation der Lehre

An einer Hochschule wurden Studierende zur Evaluation der Lehre befragt. Durch diese Unterrichtsevaluation auf der Grundlage der schriftlichen Befragung wurden sowohl Interessen von Studierenden wie auch von Lehrkräften berührt. Unter Datenschutzgesichtspunkten wäre gegen die Datenerhebung bei den Studierenden und gegen die weitere Verarbeitung dieser Daten nichts einzuwenden gewesen, wenn es zugetroffen hätte, dass die Daten anonym erhoben werden sollten, wie es der Vorbemerkung zum Fragebogen zu entnehmen war. Dann hätte die Befragung auf § 20 Abs. 3 UG gestützt werden können. Der Fragebogen war aber nicht als anonym zu bewerten. Aus den Angaben über Alter und Fächerkombination hätte z. B. bei einem älteren Studierenden ohne unverhältnismäßigen Aufwand auf dessen Person geschlossen werden können. Auch wäre die Lehrkraft zumindest unter Nutzung der freitextlichen Angaben (Handschriftenvergleich, möglicherweise aber auch aufgrund des Inhalts) in der Lage gewesen, den Personenbezug herzustellen. Für die datenschutzrechtliche Beurteilung kam es nicht darauf an, dass dies in allen Fällen gelang oder dass eine entsprechende Identifizierungsabsicht bestand, sondern es genügte, dass die Identifizierung in Einzelfällen möglich war.

Hieraus folgte, dass die Datenverarbeitung in den Anwendungsbereich des LDSG fiel und nur unter Beachtung der §§ 12 ff. LDSG zulässig war. Der Hinweis auf die Anonymität der Daten in der Vorbemerkung musste unterbleiben und da keine gesetzliche Auskunftspflicht besteht, mussten die Studierenden auf die Freiwilligkeit ihrer Angaben hingewiesen werden. Es musste ferner darauf hingewiesen werden, dass aus einer Nichtteilnahme an der Befragung keine Nachteile entstehen würden und dass die Lehrkraft auf Wunsch eine Rückmeldung über die Befragung erhalten konnte.

Auch wenn die für die Evaluation von Lehrveranstaltungen erforderlichen Informationen auf freiwilliger Grundlage erhoben wurden, bestand die Verpflichtung, den Datenschutz durch organisatorische Maßnahmen bestmöglichst zu verwirklichen. Es musste gewährleistet sein, dass die Lehrkraft keine Kenntnis vom Inhalt der Fragebögen vor deren statistischer Auswertung erhielt. Dies konnte durch eine Rückgabe im verschlossenen Umschlag erfolgen.

8.2.3 Virtueller Campus

Der Virtuelle Campus Rheinland-Pfalz (VCRP) ist eine im Aufbau befindliche gemeinsame Einrichtung der rheinland-pfälzischen Hochschulen. Er hat auf dem eigenen Server am Regionalen Hochschulrechenzentrum Kaiserslautern die Lernplattform „WebCT“ zur Durchführung Internet-basierter Lehrveranstaltungen installiert. Auf diese Lernplattform können Studierende aus ganz Rheinland-Pfalz zugreifen, wenn sie sich als solche registrieren lassen. Die Nutzung der Lernplattform ist für die Studierenden freiwillig. Das bedeutet, dass personenbezogene Daten nur aufgrund der informierten Einwilligung der Betroffenen erhoben werden. Die auf die Registrierung folgende tatsächliche Nutzung der Lernplattform ist dann als Nutzung eines Teledienstes anzusehen. In technischer Hinsicht sind die Anforderungen aus § 9 LDSG und § 4 TDDSG zugrunde zu legen. Das Verfahren wird vom LfD begleitet.

8.2.4 Webcams auf dem Campus

Eine Fachhochschule hatte ihre Absicht mitgeteilt, auf dem Campus Videokameras zu installieren. Dies nahm der LfD zum Anlass, die Umsetzung dieser Pläne im Rahmen örtlicher Feststellungen zu überprüfen. Zu diesem Zeitpunkt waren zwei Webcams installiert: eine in einem PC-Raum in einem zweiten Standort der Fachhochschule und eine auf dem Parkplatz. Die Webcam im PC-Raum diente in erster Linie zur Verhinderung möglicher Diebstähle oder Beschädigungen, da an diesem Standort keine Bediensteten der Fachhochschule anwesend waren. Eine Aufzeichnung erfolgte nicht. Die Bilder der Kamera wurden auf einen PC in der Systemadministration übertragen. Dort konnten sie bei Bedarf angesehen und auch aufgezeichnet werden. Die Bilder der Webcam oberhalb des Parkplatzes konnten nur nach technischen Vorarbeiten auf demselben Rechner eingesehen werden. Auch hier erfolgte keine Aufzeichnung. Da die Webcam über dem Parkplatz sehr hoch hing, waren einzelne Personen nur schwer erkennbar. Dennoch beabsichtigte die Fachhochschule, ein entsprechendes Hinweisschild auf die Überwachung des Parkplatzes anzubringen. Gegen den Einsatz der Webcams unter den gesehenen Bedingungen bestanden keine datenschutzrechtlichen Bedenken.

8.2.5 Bekanntgabe von Noten an der Hochschule

Im Berichtszeitraum waren immer wieder Anfragen zu beantworten, unter welchen Bedingungen Prüfungsergebnisse in der Hochschule den Studierenden bekannt gegeben werden konnten, ohne datenschutzrechtliche Bestimmungen zu verletzen.

Bei solchen Vorhaben ist sicherzustellen, dass Klausurergebnisse nicht in personenbezogener Form veröffentlicht werden, sondern dass grundsätzlich nur die Betroffenen selbst von der Bewertung Kenntnis erhalten.

Bei Aushängen in der Hochschule kann dieses Ziel durch Verwendung der Immatrikulationsnummer erreicht werden. Diese Nummer ist zwar personenbeziehbar, das dazu erforderliche Zusatzwissen ist für Unbefugte allerdings nur im Ausnahmefall und kaum aufgrund gezielter Bemühungen zu erlangen. Bei der hier anzustellenden Abwägung hält es der LfD für vertretbar, im Ergebnis bei einem solchen Verfahren unabhängig von der Anzahl der Prüflinge von einer ausreichenden Anonymisierung der Informationsweitergabe auszugehen.

Allerdings ist eine Verfahrensweise, die einen stärkeren Schutz des informationellen Selbstbestimmungsrechts der betroffenen Studierenden gewährleistet, aus datenschutzrechtlicher Sicht durchaus zu begrüßen. In diesem Zusammenhang ist z. B. die Variante, die Prüfungsergebnisse nach Zufallszahlen bekannt zu geben, datenschutzfreundlicher.

Dies gilt in gleicher Weise bei der Bereitstellung von Prüfungsergebnissen zum Abruf auf dem Hochschulserver. Soweit die pseudonymisierten Prüfungsergebnisse nur innerhalb des Campusnetzes abrufbar sind, entspricht dies einem Aushang. Bei der Übertragung im Internet ist aus datenschutzrechtlicher Sicht sicherzustellen, dass die Klausurergebnisse nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Dem kann dadurch entsprochen werden, dass die Prüfungsergebnisse in verschlüsselter Form übermittelt werden, so dass lediglich dem Betroffenen eine Kenntnisnahme möglich ist. Hinsichtlich der Stärke der kryptografischen Algorithmen ist auf die Empfehlungen im 17. Tb. Tz. 21.3.10 zu verweisen.

Asymmetrische Verfahren wie das verbreitet genutzte Programm „Pretty Good Privacy (PGP)“ eröffnen den Studierenden die Möglichkeit, geeignete Schlüssel gegebenenfalls selbst zu erzeugen und bieten Vorteile hinsichtlich des Schlüsselaustauschs. Vorrangig sollte daher eine derartige Lösung angestrebt werden.

Wenn empfängerseitig eine bestimmte Verschlüsselungssoftware nicht vorausgesetzt werden kann, kommt die Verwendung so genannter selbstextrahierender Archive in Betracht, die dem Empfänger eine Entschlüsselung auch dann ermöglicht, wenn er nicht über das vom Absender verwendete Programm verfügt. Voraussetzung hierfür ist die Vereinbarung eines Passworts. Eine Kombination aus Immatrikulationsnummer und einer Zusatzinformation (z. B. Geburtsdatum) ist in diesem Zusammenhang als ausreichend anzusehen.

Die genannten Anforderungen gelten in gleicher Weise bei der Bereitstellung von Prüfungsergebnissen zum Abruf via Internet. Auch in diesem Fall ist durch eine geeignete Verschlüsselung (z. B. SSL) und die Verwendung eines Zugangspassworts sicherzustellen, dass eine angemessene Vertraulichkeit gewährleistet wird und der Zugriff nur auf die Ergebnisse der jeweiligen Betroffenen möglich ist. Wie die Übermittlung per E-Mail ist diese Form der Bereitstellung an eine Einwilligung der Studierenden gebunden. Diese sind in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären und auf die Freiwilligkeit hinzuweisen. Die Einwilligung bedarf der Schriftform.

8.2.6 Der ewige Student

Ein Studierender bewohnte ein Appartement im Studierendenwohnheim des Studentenwerkes. Nachdem er sein Erststudium 1998 erfolgreich abgeschlossen hatte, kündigte ihm das Studentenwerk zum Herbst 2002 das Mietverhältnis. Zur Begründung hieß es, dass der Betroffene in seinem nunmehr aufgenommenen Zweitstudium – obwohl bereits im 7. Fachsemester – noch keine Prüfung abgelegt hätte, sondern vielmehr beabsichtigte, den Studiengang zu wechseln. Man wollte den kostengünstigen Wohnraum jedoch möglichst vielen Studierenden zugänglich machen. Der Studierende beschwerte sich daraufhin beim LfD darüber, dass das Studentenwerk offensichtlich Angaben über seinen Studienverlauf von der Hochschule erhalten hatte.

Das Vorgehen des Studentenwerkes war datenschutzrechtlich nicht zu beanstanden. Bei dem fraglichen Vorgang handelte es sich um eine Datenübermittlung durch die Hochschule an das rechtlich selbständige Studentenwerk. Eine solche Datenübermittlung setzt voraus, dass sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der empfangenden Stelle liegenden Aufgaben erforderlich ist und eine Datenerhebung bei Dritten zulässig wäre.

Aufgabe des Studentenwerkes ist es, die Studierenden sozial zu betreuen und wirtschaftlich und kulturell zu fördern. Hierzu gehört die Bereitstellung günstigen Wohnraums. Gefördert werden sollen in erster Linie Studierende, die noch kein Studium erfolgreich abgeschlossen haben und damit noch nicht berufsqualifiziert sind. Erst wenn deren Bedürfnisse erfüllt sind, können auch andere Studierende gefördert werden. Es war davon auszugehen, dass die Nachfrage nach Wohnheimplätzen die vorhandenen Kapazitäten überstieg. Daraus ergab sich die Erforderlichkeit, die bestehenden Mietverhältnisse zu überprüfen und jene zu kündigen, die mit nicht in erster Linie förderungswürdigen Mietern abgeschlossen waren. Da die Mietzeit des Petenten die durchschnittliche bereits weit überdauerte, lagen hier Anhaltspunkte für eine Überprüfung vor. Dies erforderte die Einholung von Informationen über den Studienverlauf. Die Kenntnis der Studiendaten war daher für die Aufgabe des Studentenwerkes erforderlich. Das Studentenwerk hatte auch zunächst versucht, die notwendigen Informationen vom Betroffenen selbst zu erlangen. Erst als dies nicht gelang, wandte man sich direkt an die Hochschule.

8.3 Forschung

8.3.1 Entschlüsselung beim Krebsregister

Im Sommer 2002 stand erstmals die Entschlüsselung von Daten des Krebsregisters im Rahmen einer europäischen multizentrischen Studie an. Das Deutsche Krebsforschungszentrum (DKFZ) in Heidelberg wollte die Assoziationen zwischen Ernährungs- und Lebensstilfaktoren und genetischer Präposition im Auftreten von Brustkrebs bei jungen Frauen untersuchen. Dazu benötigte man Daten von Patientinnen, die vor Vollendung ihres 40. Lebensjahres an Brustkrebs erkrankt waren. Zurzeit betrifft dies jährlich etwa 130 Patientinnen in Rheinland-Pfalz.

Wenn die entsprechenden Datensätze vom Krebsregister entschlüsselt worden waren, sollten die meldenden Ärzte angeschrieben und ihnen die Namen der in Frage kommenden Patientinnen mitgeteilt werden. Die Ärzte wurden sodann gebeten, den Patientinnen ein Informationsschreiben auszuhändigen. Daraus ergaben sich Ziel und nähere Umstände der Studie. Wenn eine Patientin Interesse hatte, sollte sie sich direkt mit dem DKFZ in Verbindung setzen, von dem sie dann die Unterlagen erhielt. Nach der Mitteilung an die Ärzte wurden die im Klartext vorliegenden Patientinnendaten beim Krebsregister wieder gelöscht. Da das Anschreiben an die Patientin den Hinweis auf die Freiwilligkeit der Teilnahme und darauf enthielt, dass bei Nichtteilnahme keinerlei Nachteile entstehen, wurden keine datenschutzrechtlichen Bedenken erhoben.

8.3.2 Politische Gesinnung und Naherholung

Aus der Zeitung erfuhr der LfD von einer Einwohnerbefragung, die durch eine rheinland-pfälzische Hochschule im städtischen Auftrag durchgeführt wurde. Es sollten damit Informationen zum „Wandel einer Gemeinde zwischen Landwirtschaft, Wohnort und Naherholung“ gesammelt werden. Die Fragen waren bunt gemischt. So waren Angaben vom monatlichen Gesamteinkommen bis zur politischen Grundeinstellung gefragt. Solche Erhebungen waren dann datenschutzrechtlich unbedenklich, wenn die Betroffenen zuvor umfassend über die Erhebung informiert und auf die Freiwilligkeit hingewiesen worden wären. Diese Anforderungen wurden aber nur teilweise erfüllt. Da es sich bei den Angaben zur politischen Grundeinstellung um besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 LDSG handelte, waren hier auch besondere Anforderungen zu beachten. So musste sich die Einwilligung gem. § 5 Abs. 4 LDSG ausdrücklich darauf beziehen.

9. Umweltschutz

9.1 Entwurf eines Gesetzes zur Einführung des Landesbodenschutzgesetzes

Mit Artikel 1 des Referentenentwurfs soll im Interesse der Sicherstellung eines ordnungsgemäßen Vollzuges des Bodenschutzrechts des Bundes in Rheinland-Pfalz das am 1. März 1999 in Kraft getretene Bundesbodenschutzgesetz durch die Schaffung eines Landesbodenschutzgesetzes ausgeführt und ergänzt werden. Als Folge dieses insoweit allumfassenden neuen Landesbodenschutzgesetzes werden mit Artikel 2 die altlastenrechtlichen Regelungen des bisherigen Landesabfallwirtschafts- und Altlastengesetzes aufgehoben und dieses landesgesetzliche Regelwerk auf ein reines Landesabfallwirtschaftsgesetz zurückgeführt werden. Vor diesem Hintergrund enthält das künftige Landesbodenschutzgesetz insbesondere Regelungen zu Überwachungsaufgaben und Anordnungsbefugnissen der zuständigen Behörde (§ 3), Regelungen über Mitwirkungs- und Duldungspflichten, Betretungs- und Untersuchungsrechte (§ 5) sowie Regelungen über Errichtung und Führung eines aus mehreren Fachmodulen bestehenden Bodeninformationssystems einschließlich der damit verbundenen Erfassung, Bewertung und Weitergabe von Daten (§§ 9 bis 11).

Der LfD hat anlässlich seiner Stellungnahme zum Gesetzentwurf darauf hingewiesen, dass es aus der Sicht des Datenschutzes um die Frage geht, ob und ggf. in welchem Umfang der Inhalt des Bodeninformationssystems mit Aufzeichnungen über (z. B.) Altablagerungen an andere Behörden übermittelt oder sogar veröffentlicht werden darf. Die datenschutzrechtliche Problematik ist evident: Einerseits besteht ein starkes öffentliches Interesse an möglichst breiter Information über diese Aufzeichnungen, das sich durchaus auch auf umweltbezogene Sachangaben in einer tiefen regionalen Gliederung beziehen kann. Andererseits kann die Offenbarung grundstücksbezogener – und damit personenbeziehbarer – Daten zu gravierenden Beeinträchtigungen schutzwürdiger Belange von Grundstückseigentümern führen. Für die datenschutzrechtliche Beurteilung ist weiter von Bedeutung, dass auch Hinweisdaten und andere ungesicherte Informationen (Verdachtsflächen) gespeichert werden. Wenn sich z. B. die Altlast auf einem Grundstück einer natürlichen Person befindet, handelt es sich bei den Angaben über die genaue Lage und die Flurstücksnummer der betroffenen Grundstücke regelmäßig um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes, bei deren Weitergabe das verfassungsmäßig geschützte Recht auf informationelle Selbstbestimmung zu beachten ist.

Die Regelungen in § 9 Abs. 4 und § 11 Abs. 5 des Entwurfs waren nach Auffassung des LfD datenschutzrechtlich ergänzungsbedürftig. So sollte beispielsweise der Grundsatz der Erhebung beim Betroffenen aufgenommen werden. Im Interesse einer Verdeutlichung der datenschutzrechtlichen Zusammenhänge wurde angeregt, den Datenschutz in einer entsprechenden Bestimmung zu regeln, die wie folgt aussehen könnte:

„Datenschutz

(1) Die zuständige Behörde ist berechtigt, die zum Zwecke der Aufgabenerfüllung nach diesem Gesetz, dem Bundesbodenschutzgesetz sowie der aufgrund dieser Gesetze erlassenen Rechtsverordnungen erforderlichen Daten zu erheben und weiter zu verarbeiten.

(2) Personenbezogene Daten im Sinne von § 3 Abs. 1 Landesdatenschutzgesetz sind grundsätzlich bei den Betroffenen zu erheben. Werden personenbezogene Daten nicht bei den Betroffenen erhoben, so hat die erhebende Stelle die Betroffenen von der Speicherung sowie über die Zweckbestimmung der Verarbeitung zu unterrichten. Die Unterrichtung erfolgt bei der ersten Übermittlung. Eine Pflicht zur Benachrichtigung besteht nicht, wenn
1. die Betroffenen auf andere Weise von der Speicherung oder der Übermittlung Kenntnis erlangt haben,
2. die Unterrichtung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde oder
3. die Speicherung oder Übermittlung der Daten aufgrund eines Gesetzes ausdrücklich vorgesehen ist.

(3) Die zuständigen Behörden dürfen personenbezogene Daten an öffentliche Stellen übermitteln, soweit diese Aufgaben des Umweltschutzes, insbesondere solche der Information, der Vorsorge, der Überwachung, der Gefahrenabwehr oder der Schadensbeseitigung wahrnehmen und die Daten zur Erfüllung dieser Aufgaben erforderlich sind.

(4) Soweit die zuständigen Behörden Angaben aus dem Bodeninformationssystem der Öffentlichkeit zugänglich machen, darf die Bekanntgabe keine personenbezogenen Daten (§ 3 Abs. 1 Landesdatenschutzgesetz) enthalten. Dies gilt nicht, wenn solche Angaben offenkundig sind oder ihre Bekanntgabe zur Abwehr von Gefahren oder aus anderen überwiegenden Gründen des Wohls der Allgemeinheit erforderlich ist.“

Zwischenzeitlich hat das Umweltministerium mitgeteilt, dass es den Formulierungsvorschlag des LfD in den Gesetzentwurf übernehmen wird.

9.2 Entwurf eines Gesetzes zur Änderung des Landeswassergesetzes

Der Gesetzentwurf dient in erster Linie der Umsetzung der „Wasser-Rahmenrichtlinie“ des Europäischen Parlaments und des Rates vom 23. Oktober 2000 zur Schaffung eines Ordnungsrahmens für Maßnahmen der Gemeinschaft im Bereich der Wasserpolitik in das Recht des Landes Rheinland-Pfalz. Außerdem wurden eine Reihe von Änderungen als Schlussfolgerungen aus Rechtsprechung und Vollzugserfahrungen eingearbeitet.

In seiner Stellungnahme konnte der LfD den im Referentenentwurf enthaltenen datenschutzbezogenen Aussagen im Wesentlichen zustimmen, wobei er auf Folgendes aufmerksam gemacht hat:

Aus der Sicht des Datenschutzes geht es um die Sicherung des Rechts auf informationelle Selbstbestimmung. Umweltbezogene Informationen können sensible personenbezogene Daten enthalten. Das Bundesverfassungsgericht hat in seiner grundlegenden Entscheidung zum Grundrecht auf informationelle Selbstbestimmung aus dem mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleisteten Recht die Befugnis des Einzelnen abgeleitet, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Eine Einschränkung dieses informationellen Selbstbestimmungsrechts ist nur bei überwiegendem Allgemeininteresse zulässig und bedarf einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzung und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind zulässig, weil das Recht im Hinblick auf die Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person nicht schrankenlos gewährleistet ist. Dem Gemeinschaftsinteresse kann also unter bestimmten Voraussetzungen Vorrang vor dem Einzelinteresse eingeräumt werden.

Dies ist nach Auffassung des LfD mit § 109 a des vorliegenden Entwurfs in zulässiger Weise und innerhalb der vom Bundesverfassungsgericht gesetzten Grenzen erfolgt. Vorkehrungen zur Missbrauchssicherung sind durch die Festlegung der Zwecke und durch den ausdrücklich noch einmal aufgenommenen Grundsatz der Erforderlichkeit sowie durch den Verweis auf die ergänzende Geltung der Vorschriften des Landesdatenschutzgesetzes in hinreichender Weise getroffen. Was die Zulassung der Datenerhebung ohne Kenntnis der Betroffenen anbelangt, so regelt § 109 a Abs. 1 Satz 2 des Entwurfs ausdrücklich, dass solche Datenerhebungen nur dann erfolgen dürfen, wenn andernfalls die Erfüllung der nach Satz 1 genannten Aufgaben gefährdet würde.

Ergänzungsbedürftig waren aus Sicht des LfD allerdings die Ausführungen im Begründungsteil zu § 109 a. Im Interesse einer Verdeutlichung der datenschutzrechtlichen Zusammenhänge hat er angeregt, klarstellend Folgendes auszuführen:

„Diese spezialgesetzliche Regelung zum Umgang mit Daten im Bereich des rheinland-pfälzischen Wassergesetzes bildet nach Absatz 2 die Rechtsgrundlage für die Erhebung personenbezogener Daten im Sinne von § 3 Abs. 1 des rheinland-pfälzischen Landesdatenschutzgesetzes vom 5. Juli 1994 (GVBl. S. 293, zuletzt geändert durch Gesetz vom 8. Mai 2002, GVBl. S. 177) zum Zwecke der in Absatz 1 beschriebenen Aufgabenerfüllung. Personenbezogene Daten sind grundsätzlich bei den Betroffenen zu erheben. Dieser Grundsatz lässt sich im Verwaltungsvollzug nicht immer aufrechterhalten. Abs. 1 Satz 2 stellt eine Ausnahmeregelung dar, wobei nach Maßgabe der Voraussetzungen des rheinland-pfälzischen Landesdatenschutzgesetzes (vgl. Abs. 4) Ausnahmen zugelassen werden, wenn andernfalls die Erfüllung der nach Abs. 1 Satz 1 genannten Aufgaben gefährdet würde."

Der dem Parlament vorgelegte Gesetzentwurf (Landtagsdrucksache 14/2300) enthält nunmehr die angeregten Klarstellungen.

9.3 Digitales Wasserbuch

Bei den beiden Struktur- und Genehmigungsdirektionen als oberer Wasserbehörde werden die sog. Wasserbücher geführt, ein öffentliches Register aller erteilten Wasserrechte. Die Führung richtet sich nach der einschlägigen Verwaltungsvorschrift aus dem Jahre 1987 und erfolgt gegenwärtig im Wesentlichen über Karteikarten. Die Einsichtnahme in das Wasserbuch und diejenigen wasserrechtlichen Entscheidungen, auf die Bezug genommen wird, ist gem. § 127 Landeswassergesetz jedermann gestattet. Das Projekt „Digitales Wasserbuch" zielt darauf ab, die Wasserbücher in eine EDV-Datenbankanwendung zu überführen, wobei daran gedacht wurde, das Wasserbuch über das Internet auch unmittelbar der Öffentlichkeit zugänglich zu machen.

Im Interesse einer Verdeutlichung der rechtlichen Zusammenhänge war im Rahmen der Stellungnahme des LfD auf Folgendes hinzuweisen:

Grundsätzlich begründen die Rechtsvorschriften, die den Zugang zu Informationen über die Umwelt regeln, ein subjektiv-öffentliches Recht auf Zugang zu analogen und digitalen Aufzeichnungen. Das Recht auf Einsichtnahme wird nur durch Vorschriften über Geheimhaltung und Datenschutz eingeschränkt (vgl. § 127 Satz 3 Landeswassergesetz).

Nach § 4 Abs. 1 Satz 1 UIG haben natürliche Personen und juristische Personen des privaten Rechts ein Recht auf Zugang zu Informationen über die Umwelt, die von einer öffentlichen Stelle, der Aufgaben des Umweltschutzes obliegen, gespeichert werden. Der Schutz privater Interessen richtet sich nach § 8 Abs. 1 und 3 UIG. Aufzeichnungen, die dem Datengeheimnis unterliegen oder Betriebs- und Geschäftsgeheimnisse enthalten, dürfen nur dann zugänglich gemacht werden, wenn sich aus der Abwägung des Interesses am Datenschutz mit dem Interesse am Datenzugang ein Vorrang des Letzteren ergibt. Die Entscheidung, in welcher Form der Zugang eröffnet wird, liegt gem. § 4 Abs. 1 Satz 2 UIG im Ermessen der öffentlichen Stelle.

Soweit über das digitale Wasserbuch und das Grundbuch natürliche Personen als konkrete Grundstückseigentümer bestimmbar sind, erfolgt die Verarbeitung oder Nutzung der Daten personenbezogen. Die Zulässigkeit einer Veröffentlichung dieser Daten erfordert nach § 8 UIG eine Abwägung im Einzelfall unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen.

Daraus ergibt sich, dass bei einer Veröffentlichung personenbezogener (bzw. personenbeziehbarer) Daten im digitalen Wasserbuch die Vorgaben des § 8 UIG – insbesondere auch bei einem Zugriff über das Internet – einzuhalten sind. In diesem Zusammenhang stand allerdings zu fragen, wie die Berücksichtigung der schutzwürdigen Belange der Betroffenen hier erfolgen sollte.

Das Umweltministerium hat die Hinweise des LfD zum Anlass genommen, die Konzeption für das digitale Wasserbuch anzupassen. Dementsprechend ist vorgesehen, personenbezogene Daten vollständig aus dem Internet-Angebot herauszunehmen. Dies gilt für alle Wasserrechte, die natürliche Personen als Rechtsinhaber ausweisen. Das Internet-basierte Informationsangebot wird daher lediglich eine Beschreibung der Rechtstitel nach Art, Umfang, Lage und Dauer enthalten, die keine Rückschlüsse auf Rechtsinhaber enthält.

10. Gesundheitswesen

10.1 Patientenquittung

In einem bundesweit einmaligen Modellprojekt hatten Versicherte im Zuständigkeitsbereich der Kassenärztlichen Vereinigung Rheinhessen die Möglichkeit, sich über die in ihrem Fall ärztlich abgerechneten Leistungen zu informieren. Die Patienten erhielten auf Wunsch bei den teilnehmenden rund 100 Ärzten unterschiedlicher Fachrichtungen eine Aufstellung über Behandlungen und ihre Kosten. Die Ärzte erstellten die „Quittung“ entweder nach jedem Besuch oder am Ende eines Abrechnungsquartals. Das Modellprojekt war eine gemeinsame Initiative der Kassenärztlichen Vereinigung Rheinhessen, der Kassenärztlichen Bundesvereinigung, der Krankenkassen in Rheinland-Pfalz und des Ministeriums für Arbeit, Soziales, Familie und Gesundheit, welche damit auch unterschiedliche Erwartungen verbanden. So versprach sich das Ministerium, dass der Versicherte stärker in die Behandlung einbezogen und zu einem mündigen und aufgeklärten Partner des Arztes werden sollte. Nach den zahlreichen Ermittlungsverfahren wegen Abrechnungsbetrügereien ging das Interesse der Kassenärztlichen Vereinigung dahin, das Image der Ärzte zu verbessern. Die Krankenkassen, die das Projekt mit 750 000 € finanzierten, erhofften sich mit der verbesserten Transparenz auch mehr Kostenbewusstsein bei den Versicherten.

Auch datenschutzrechtlich ist die Unterrichtung der Versicherten über die ärztlich abgerechneten Leistungen ausdrücklich zu unterstützen. Im 17. Tb (Tz. 11.5.3) hatte der LfD letztmals darauf hingewiesen, dass der diesbezügliche Auskunftsanspruch der Versicherten gem. § 305 Abs. 2 SGB V aus Kostengründen seitens der Kassenärztlichen Vereinigungen contra legem bislang nicht umgesetzt wurde.

Da die Patientenquittung nach dem Willen der Bundesregierung bundesweit eingeführt werden soll, ermittelte das Zentralinstitut für die Kassenärztliche Versorgung im Rahmen der wissenschaftlichen Begleitung Aufwand, Praktikabilität und Akzeptanz der Patienteninformation. Diese ergab, dass über 80 % der Patienten, welche im Rahmen der wissenschaftlichen Begleitung einen Fragebogen beantwortet hatten, es für wichtig halten, ärztliche Leistungen nachvollziehen zu können. Gleichwohl wird man bei einer bundesweiten Einführung zu berücksichtigen haben, dass das Interesse der Patienten im Verlauf des Modellversuchs kontinuierlich gesunken ist. Während anfangs noch 22 % eine Quittung verlangten, waren es im letzten von vier Quartalen nur 8 %.

Der LfD wird die weitere Entwicklung, insbesondere die von Seiten der Bundesregierung angestrebte Integration der Patientenquittung auf einer elektronischen Gesundheitskarte, weiterhin kritisch begleiten.

10.2 Erhebungsbogen bei amtsärztlichen Untersuchungen

Die Erhebung von personenbezogenen Daten im Zusammenhang mit amtsärztlichen Untersuchungen war im Berichtszeitraum häufiger Gegenstand von Eingaben an den LfD. Problematisiert wurde in erster Linie der Einsatz von einheitlichen Erhebungsbögen. Da diese in ganz unterschiedlichen Zusammenhängen (z. B. Einstellungsuntersuchung, Überprüfung zur Eignung zum Führen eines Kfz im Straßenverkehr, Überprüfung einer Arbeitsunfähigkeitsbescheinigung) verwendet werden und deshalb pauschal und sehr umfassend Informationen einholen, stand für die Betroffenen oftmals der Umfang der Datenerhebung im Verhältnis zu dem konkreten Untersuchungszweck in keinem nachvollziehbaren Zusammenhang mehr (Beispiel: weitreichende Angaben zur Familienanamnese – psychische Krankheiten/Selbstmordversuche u. Ä. – im Zusammenhang mit einer Begutachtung zur Reduzierung der Arbeitszeit).

Zu dem Einsatz einheitlicher Erhebungsbögen bei amtsärztlichen Untersuchungen und den daraus resultierenden datenschutzrechtlichen Problemen hatte der LfD bereits in seinem 15. Tb. (Tz. 10.2.2) Stellung genommen. Trotz der darin angekündigten Bemühungen des LfD, sich bei den Gesundheitsämtern für die Durchführung individueller und an dem Erforderlichkeitsgrundsatz orientierter Befragungen einzusetzen, wurden auch weiterhin im Zusammenhang mit amtsärztlichen Untersuchungen verbreitet routinemäßige Datenerhebungen durchgeführt. Aus diesem Grunde wandte sich der LfD nun erneut an das Ministerium für Arbeit, Soziales, Familie und Gesundheit mit der Bitte, die Gesundheitsämter auf die bestehende Rechtslage hinzuweisen. Dieser Bitte kam das Ministerium auch umgehend nach.

Zentraler Gesichtspunkt ist die Erforderlichkeit der Datenerhebung bzw. Datenspeicherung zur rechtmäßigen Erfüllung der Aufgaben der Behörden des öffentlichen Gesundheitsdienstes (vgl. § 11 Abs. 2 ÖGdG; § 12 Abs. 1 LDSG). Dies bedeutet, dass im Einzelfalle bei einer Untersuchung durch das Gesundheitsamt nur diejenigen Daten erhoben werden dürfen, die zur Erfüllung des konkreten Untersuchungsauftrages zwingend erforderlich sind. Der Einsatz umfänglicher einheitlicher Fragebögen bei amtsärztlichen Untersuchungen ist deshalb datenschutzrechtlich problematisch und sollte grundsätzlich unterbleiben. Vielmehr sollten die für den konkreten Untersuchungszweck notwendigen Fragen im Gespräch mit dem Amtsarzt erhoben werden. Alternativ kommt bei dem Einsatz von Erhebungsbögen auch in Betracht, die Betroffenen in einem gesonderten Hinweisblatt auf die Möglichkeit aufmerksam zu machen, bestimmte Fragen direkt mit dem untersuchenden Arzt zu klären.

Soweit es für die konkrete Datenverarbeitung auf die Einwilligung der Betroffenen ankommt, sind die in den §§ 11 Abs. 2 Satz 2 ÖGdG i. V. m. 5 Abs. 2 bis 4 LDSG enthaltenen Anforderungen zu beachten. Da die Daten über die Gesundheit nach § 3 Abs. 9 LDSG als sog. „besondere Arten personenbezogener Daten“ einen besonderen Schutz genießen, muss sich die Einwilligungserklärung ausdrücklich auf sie beziehen. Die Betroffenen sind in geeigneter Weise über die Bedeutung der Einwilligung, deren Widerrufsmöglichkeit, den vorgesehenen Zweck der Verarbeitung, den möglichen Empfängerkreis und die verantwortliche Stelle aufzuklären. Auch hinsichtlich der Einwilligungserklärungen sollte angesichts der vielfältigen Zwecke der amtsärztlichen Untersuchungen grundsätzlich von der Verwendung einheitlicher Standardformulierungen abgesehen werden.

10.3 Falschübermittlung von Patientendaten per Fax

Die Tücken der modernen Kommunikationsmittel belegte sehr anschaulich die Eingabe eines niedergelassenen Arztes, der sich gegenüber dem LfD darüber beklagte, dass er schon seit geraumer Zeit von diversen Geschäftsstellen einer Krankenkasse höchst sensible Patientendaten per Fax in seine Privatwohnung übermittelt bekommen habe. Er vermutete, dass ein sog. Zahlendreher für die wiederholte Falschübermittlung der Dokumente – hauptsächlich Privatliquidationen und Rezepte im Zusammenhang mit Impfungen – verantwortlich war. Seine Versuche, den Missstand abzustellen und zu veranlassen, dass die Irrläufer durch Mitarbeiter der Krankenkasse abgeholt werden sollten, blieben zu seinem Erstaunen jedoch ohne Reaktion.

Leider konnte erst durch die Einschaltung des LfD erreicht werden, dass das Versenden der Unterlagen per Fax unverzüglich eingestellt wurde. Angesichts dieser Vorkommnisse empfiehlt der LfD noch einmal eindringlich, bei der Übersendung von Dokumenten, die besonders geschützte personenbezogene Daten enthalten (z. B. Gesundheits-, Sozial-, Personalakten-, Steuerdaten, Daten i. S. v. § 3 Abs. 9 LDSG), diese grundsätzlich nicht per Telefax zu übertragen, da hierbei die Gefahr eines Übermittlungsfehlers und der damit verbundenen unbefugten Datenweitergabe – wie der aktuelle Fall zeigte – nicht von der Hand zu weisen ist. Jedenfalls sollten die in der Orientierungshilfe „Datenschutz und Telefax“ (abrufbar über www.datenschutz.rlp.de) aufgeführten Grundsätze zur Vermeidung von Faxirrläufern strikt eingehalten werden.

10.4 In letzter Sekunde – Gesundheitsmodernisierungsgesetz

Kurz vor Ablauf des Berichtszeitraums wurde im September 2003 der zwischen den Bundestagsfraktionen erzielte Kompromiss zur Gesundheitsreform im Bundestag verabschiedet. Es ist davon auszugehen, dass der Gesetzentwurf in der vom Parlament beschlossenen Form umgesetzt und zu Beginn des Jahres 2004 in Kraft treten wird.

Aus datenschutzrechtlicher Sicht muss das Reformwerk differenziert beurteilt werden. Die diesbezügliche Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003 (vgl. Anlage 26) spiegelt dies wider und benennt zugleich deutlich die Gefahr, die die Datenschutzbeauftragten in dem Gesundheitsmodernisierungsgesetz sehen: die Gefahr des gläsernen Patienten. Es liegt letztendlich in der Verantwortung aller beteiligten Akteure, ob sich diese Gefahr auch tatsächlich realisieren wird. Die Notwendigkeit einer kritischen Begleitung durch die Datenschutzbehörden liegt jedenfalls schon jetzt auf der Hand.

11. Datenschutz bei Sozialleistungsträgern

11.1 Datenschutz im Jugendamt – Informationsansprüche der Pflegeeltern

Ein Jugendamt bat um eine Stellungnahme zu der Frage, ob es Informationen über die leiblichen Eltern eines Kindes an die Pflegeeltern weitergeben darf, damit diese ihr Pflegekind zu gegebener Zeit über die Hintergründe seiner familiären Situation informieren können. Im konkreten Fall hatten die drogenabhängigen leiblichen Eltern des Kindes jeglichen Kontakt zu Jugendamt und Pflegeeltern abgebrochen, nachdem ihnen das Sorgerecht entzogen und Amtsvormundschaft angeordnet worden war.

Rechtsgrundlage für die Weitergabe von Informationen über die leiblichen Eltern ist § 68 SGB VIII. Abs. 1 dieser Vorschrift setzt voraus, dass eine Datenübermittlung zur Erfüllung der Aufgabe als Amtsvormund erforderlich sein muss. Hierbei ist zu beachten, dass § 68 Abs. 3 SGB VIII und § 61 Abs. 2 PStG einen Auskunftsanspruch lediglich des Betroffenen hinsichtlich seiner eigenen Abstammung ab einer bestimmten Altersgrenze beinhalten. Dieser besteht nur insoweit, als berechtigte Interessen Dritter dem Auskunftsanspruch nicht entgegenstehen.

Diese Auskunftsansprüche des Betroffenen in Bezug auf seine eigene Abstammung sind auf die Pflegeeltern jedenfalls nicht übertragbar. Aufgrund der bestehenden Amtsvormundschaft können die Pflegeeltern die Ansprüche des Kindes auch nicht im Wege der gesetzlichen Vertretung geltend machen. Die Pflegeeltern haben daher jedenfalls keinen Anspruch auf nähere Informationen über die leiblichen Eltern ihres Pflegekindes.

Bei der Frage, ob die Informationsweitergabe zur Aufgabenerfüllung der Person, der die Amtsvormundschaft im Jugendamt übertragen ist, erforderlich ist, ist zu berücksichtigen, über welche Informationen die Pflegeeltern bereits jetzt verfügen und ob diese Informationen zur Aufklärung über den familiären Hintergrund bis zur möglichen Ausübung eigener Auskunftsansprüche ausreichen. Der Umfang der Unterrichtung der Pflegeeltern durch das Jugendamt darf jedenfalls die Grenze des § 68 Abs. 3 SGB VIII nicht überschreiten, d. h. die Drogenabhängigkeit der leiblichen Eltern ist als ein der Auskunftserteilung möglicherweise entgegenstehendes berechtigtes Drittinteresse zu berücksichtigen.

11.2 Routinemäßige Grundbuchanfragen durch die Sozialämter

Im Rahmen einer behördlichen Anfrage hatte der LfD die Frage zu beurteilen, ob bei der Durchführung von Verfahren nach dem BSHG bzw. GSiG das routinemäßige Einholen von Auskünften beim Grundbuchamt mit den datenschutzrechtlichen Bestimmungen noch zu vereinbaren ist. Hintergrund der Eingabe war die Vermutung der Behörde, dass es bei der Bearbeitung von Anträgen auf Hilfe zum Lebensunterhalt bzw. auf Leistungen nach dem GSiG bei manchen Verwaltungen üblich sei, grundsätzlich ein Amtshilfeersuchen an das örtlich zuständige Grundbuchamt einzureichen, um in Erfahrung zu bringen, ob die Antragsteller über Grund- oder Wohneigentum verfügen, welches eventuell im Antrag auf Sozialhilfe bzw. Grundsicherung verschwiegen wurde. Die Behörde hatte Bedenken, ob diese Anfragen ohne Vorliegen konkreter Anhaltspunkte und ohne Wissen der Betroffenen datenschutzrechtlich zulässig sind.

In Übereinstimmung mit dem Ministerium für Arbeit, Soziales, Familie und Gesundheit vertritt der LfD die Auffassung, dass unter Berücksichtigung der zugrunde liegenden Rechtsgrundlagen, insbesondere der §§ 67 a Abs. 2 Satz 2 Nr. 2 SGB X und 60 Abs. 1 Nr. 1 SGB I, sowie angesichts der Rechtsprechung des Hessischen VGH zur Einholung von Bankauskünften in Sozialhilfeverfahren (Beschluss vom 7. Februar 1995, DVBl. 1995 S. 702 f.), routinemäßige Grundbuchanfragen im Rahmen der Durchführung der o. g. Verfahren angesichts der bereits von den Antragstellern in den Anträgen hierzu gemachten Angaben grundsätzlich nicht erforderlich und damit datenschutzrechtlich unzulässig sind. Lediglich dann, wenn wegen des Vorliegens konkreter Anhaltspunkte eine weitere Sachverhaltsaufklärung nur in Form einer Grundbuchanfrage möglich ist, wäre diese auch erforderlich i. S. v. § 67 a Abs. 2 Satz 2 Nr. 2 b SGB X und damit zulässig.

11.3 Plausibilitätsprüfungen gem. § 83 Abs. 2 SGB V mit Kassenvertretern

Der LfD wurde von zwei Kassenärztlichen Vereinigungen um eine Stellungnahme zu der Frage gebeten, ob datenschutzrechtliche Bedenken dagegen bestehen, an den Plausibilitätsprüfungen gem. § 83 Abs. 2 SGB V (auch künftig) Vertreter der Krankenkassen zu beteiligen bzw. – hierüber hinausgehend – Patientenbefragungen durch die Krankenkassen durchzuführen. In einer gemeinsamen Besprechung wurde vorgetragen, dass sich der gegenseitige Informationsaustausch zwischen Kassenärztlichen Vereinigungen und Krankenkassen innerhalb der Plausibilitätskommission aus Sicht der Beteiligten bewährt habe. Das Verfahren sollte daher nach dem Willen des Ministeriums für Arbeits, Soziales, Familie und Gesundheit landesweit eingeführt werden.

Bei der Frage, ob ein Erfordernis besteht, Patientendaten in personenbezogener Form zu erheben und zu verarbeiten, bestand unter den Beteiligten indes Einvernehmen darüber, dass die Plausibilitätskommission ihre Aufgaben künftig auch ohne namentliche Benennung der Patienten erfüllen kann, wodurch Patientenbefragungen damit künftig grundsätzlich ausgeschlossen sind. Der Verzicht auf die Erhebung und Verarbeitung personenbezogener Patientendaten für Zwecke der Plausibilitätsprüfung entspricht nunmehr der Regelung in § 285 Abs. 2 SGB V, wonach die Kassenärztlichen Vereinigungen berechtigt sind, nur im erforderlichen Umfang versichertenbezogene Daten im Rahmen von Plausibilitätsprüfungen zu erheben und zu speichern.

Im Übrigen bewertete der LfD die Teilnahme der Krankenkassenvertreter an den Sitzungen der Plausibilitätskommission wie folgt:

Angesichts des Ziels der Plausibilitätsprüfungen, möglicherweise fehlerhafte ärztliche Abrechnungen aufzudecken, ist davon auszugehen, dass auch Krankenkassen durch ihre Versicherten im Einzelfall über sachdienliche Informationen in Bezug auf das Abrechnungsverhalten einzelner Vertragsärzte verfügen können, so dass die Beteiligung von Vertretern der Krankenkassen zunächst nachvollziehbar ist. Eine datenschutzrechtliche Prüfung hat sich jedoch streng an den einschlägigen datenschutzrelevanten Bestimmungen zu orientieren und kann daher weder den Erfolg noch die Sinnhaftigkeit eines Verfahrens in den Mittelpunkt der Betrachtung stellen.

Gemäß § 83 Abs. 2 SGB V sind in den Gesamtverträgen auch Verfahren zu vereinbaren, die die Prüfung der Abrechnung auf Rechtmäßigkeit durch Plausibilitätskontrollen der Kassenärztlichen Vereinigungen ermöglichen. Der Wortlaut der Vorschrift legt nahe, dass es die alleinige Aufgabe der Kassenärztlichen Vereinigungen ist, Plausibilitätsprüfungen vorzunehmen. Dementsprechend sehen die §§ 45 f BMV-Ä sowie 34 BMV-Ä/EK vor, dass den Kassenärztlichen Vereinigungen die Prüfung der von den Vertragsärzten

vorgelegten Abrechnungen ihrer vertragsärztlichen Leistungen obliegt. Vieles spricht daher dafür, dass die Durchführung der Plausibilitätskontrollen ausschließlich in den Zuständigkeitsbereich der Kassenärztlichen Vereinigungen fällt (so auch Hauck/Klückmann, Kommentar zum SGB V, § 83 RnNr. 7 und 9). Dies ist auch der Rechtsprechung des BSG zur Unterscheidung zwischen Wirtschaftlichkeitsprüfungen einerseits und sachlich-rechnerischen Prüfungen andererseits zu entnehmen. Eine Plausibilitätskontrolle in der Form einer sachlich-rechnerischen Berichtigung des Honoraranspruchs wird hiernach auch im Rahmen von Wirtschaftlichkeitsprüfungen u. a. dann für zulässig gehalten, wenn der Frage der Berechnungs- und Verordnungsfähigkeit im Verhältnis zur Wirtschaftlichkeit keine derart überragende Bedeutung zukommt, dass eine Abgabe an die Kassenärztliche Vereinigung geboten wäre (NJW 1996, 3101 f.).

Dem steht nicht entgegen, dass die den Kassenärztlichen Vereinigungen nach § 75 Abs. 1 SGB V obliegende Verpflichtung zur Gewährung einer den gesetzlichen und vertraglichen Erfordernissen entsprechenden vertragsärztlichen Versorgung nach der Auffassung des BSG nicht im Sinne einer prinzipiellen Alleinzuständigkeit zu interpretieren sei, sondern das Gesetz vielmehr im Grundsatz von einer gemeinsamen Erfüllung der bei der Durchführung und Überwachung der vertragsärztlichen Versorgung anfallenden Aufgaben durch Krankenkassen und Kassenärztliche Vereinigungen ausgehe (vgl. BSGE 69, 154, 157). Denn allein aus der Zuständigkeit kann nicht auf die Befugnis der Krankenkassen geschlossen werden, in das informationelle Selbstbestimmungsrecht der Betroffenen einzugreifen. Nach der Rechtsprechung des Bundesverfassungsgerichtes (BVerfGE 65, 1) bedarf es hierfür einer normenklaren gesetzlichen Grundlage. Dies gilt auch für die Erhebung und Verarbeitung von arztbezogenen Daten, selbst wenn man diese nicht als „Sozialdaten“ oder als nicht „schützenswerte höchstpersönliche Daten“ qualifiziert (vgl. BVerfG, Beschluss vom 10. April 2000, NJW 2001, S. 883 f.).

Im Zusammenhang mit der Durchführung von Plausibilitätsprüfungen sind ausdrückliche Bestimmungen jedoch lediglich im Zusammenhang mit der Informationsverarbeitung durch die Kassenärztlichen Vereinigungen vorhanden: So regelt beispielsweise § 295 Abs. 1 a SGB V die Verpflichtung der Ärzte, auf Verlangen der Kassenärztlichen Vereinigung die für die Prüfung nach § 83 Abs. 2 SGB V erforderlichen Befunde vorzulegen. § 285 Abs. 1 Ziff. 2 und Abs. 2 SGB V regeln die Befugnis der Kassenärztlichen Vereinigungen, arzt- bzw. versichertenbezogene Daten zur Überprüfung der Zulässigkeit und Richtigkeit der Abrechnung zu erheben und zu speichern, soweit diese für die Aufgabenerfüllung nach § 83 Abs. 2 SGB V erforderlich sind. Ausdrückliche Rechtsvorschriften, welche die Datenerhebung und -verarbeitung durch die Krankenkassen im Zusammenhang mit Plausibilitätsprüfungen zum Gegenstand haben, sind indes dem SGB V nicht zu entnehmen.

Aus den dezidierten Regelungen zum Datenaustausch zwischen Kassenärztlichen Vereinigungen und Krankenkassen (vgl. §§ 296, 297 SGB V) im Zusammenhang mit Wirtschaftlichkeitsprüfungen und dem Fehlen entsprechender Bestimmungen für Plausibilitätskontrollen kann daher geschlossen werden, dass der Gesetzgeber eine Beteiligung der Krankenkassenvertreter an Plausibilitätsprüfungen unter Kenntnisnahme personenbezogener Daten nicht gewollt hat.

§ 284 Abs. 1 Ziff. 8 SGB V legitimiert zwar die Krankenkassen, Sozialdaten zu erheben und zu speichern, soweit diese für die Abrechnung mit den Leistungserbringern erforderlich sind. Eine Legitimation zur Beteiligung an Plausibilitätsprüfungen kann daraus jedoch nicht geschlossen werden: Zum einen verwendet der Gesetzgeber in Bezug auf die Kassenärztlichen Vereinigungen, deren Kompetenz zur Überprüfung der Rechtmäßigkeit der Abrechnung unstreitig ist, in § 285 Abs. 1 Ziff. 2 SGB V eine völlig andere und viel konkretere Formulierung, zum anderen enthält § 294 Abs. 1 Ziff. 9 SGB V eine ausdrückliche Datenerhebungsbefugnis der Krankenkassen im Zusammenhang mit Wirtschaftlichkeitsprüfungen nach § 106 SGB V. Hätte der Gesetzgeber eine entsprechende Befugnis der Krankenkassen im Zusammenhang mit Plausibilitätsprüfungen angenommen, hätte er dies in diesem Zusammenhang ebenso spezialgesetzlich ausgestaltet.

Selbst wenn man eine Datenerhebungsbefugnis der Krankenkassen für Plausibilitätsprüfungen gem. § 284 Abs. 1 Ziff. 8 SGB V unterstellt, ist zu beachten, dass diese nur eine auf den Einzelfall bezogene, sich streng am Erforderlichkeitsgrundsatz zu orientierende Informationsbeschaffung legitimiert. Gleiches gilt für die bestehende Befugnis der Krankenkassen, einzelfallbezogen einer Kassenärztlichen Vereinigung Hinweise über eine möglicherweise unplausible Abrechnung eines Vertragsarztes zu geben. Auch ist eine Kassenärztliche Vereinigung nicht gehindert, im Einzelfall arztbezogene Daten bei einer Krankenkasse anzufordern. Auch die Vertragspartner des Bundesmantelvertrages Ärzte sind ausweislich der Regelung in § 46 Satz 2 von einer einzelfallbezogenen Beteiligung der Krankenkassen ausgegangen.

Durch die Teilnahme an Sitzungen der Plausibilitätskommission soll aber ein deutlich weiter gehender Zweck, nämlich der eines freien Informationsaustausches zwischen Krankenkassen und Kassenärztlichen Vereinigungen, der sich gerade nicht auf das Notwendige im Einzelfall zu beschränken hat, gefördert werden. Die Krankenkasse erhält dabei beispielsweise Kenntnis davon, ob und wie gegenüber einem auffällig gewordenen Arzt – bis hin zur Einschaltung von Polizei und Staatsanwaltschaft – vorgegangen wird, auch wenn diese nicht selbst den Anstoß zu einer Abrechnungsprüfung gegeben hat und auch zur Sachaufklärung nichts beitragen konnte.

Insgesamt geht der Informationsaustausch damit deutlich über eine einzelfallbezogene Datenerhebung und -verarbeitung hinaus, ohne dass hierfür eine Rechtsgrundlage ersichtlich wäre.

Die Kassenärztlichen Vereinigungen teilten nach Unterrichtung über die Rechtsauffassung des LfD mit, Plausibilitätsprüfungen künftig ohne Kassenvertreter vornehmen zu wollen.

11.4 Akteneinsicht des Bevollmächtigten im Verfahren zur Durchführung von Plausibilitätskontrollen

In einer Anfrage hatte der LfD zu klären, ob dem Rechtsanwalt eines Arztes im Rahmen der Durchführung eines Plausibilitätsverfahrens durch die Kassenärztliche Vereinigung Akteneinsicht gewährt werden darf.

Bei der Gewährung von Akteneinsicht in den o. g. Fällen werden regelmäßig personenbezogene Daten nicht nur des von der Prüfung betroffenen Arztes, sondern auch von dessen Patienten übermittelt. Soweit es um die den Arzt betreffenden personenbezogenen Daten geht, ist von dessen Einwilligung in die Datenübermittlung an seinen Bevollmächtigten auszugehen. Soweit dagegen die in den Unterlagen enthaltenen Patientendaten betroffen sind, hängt die datenschutzrechtliche Zulässigkeit mangels Einwilligung von dem Vorliegen einer entsprechenden Erlaubnisvorschrift ab.

Rechtsgrundlage des Plausibilitätsverfahrens zur Prüfung der Rechtmäßigkeit der vertragsärztlichen Abrechnungen ist § 83 Abs. 2 SGB V i. V. m. § 46 BMV-Ä bzw. § 42 BMV-Ä/EK sowie den im Bereich der jeweiligen Kassenärztlichen Vereinigung geschlossenen gesamtvertraglichen Vereinbarungen. Diese Regelungen enthalten jedoch keine Aussagen über die Ausgestaltung des Verfahrens bzw. der den betroffenen Vertragsärzten zustehenden Verfahrensrechte. Diesbezüglich war vielmehr die Verfahrensordnung zur Durchführung von Plausibilitätsprüfungen nach § 83 Abs. 2 i. V. m. § 75 Abs. 1 SGB V im Bereich der anfragenden Kassenärztlichen Vereinigung heranzuziehen, zumal es nach dem gesetzgeberischen Willen (§ 83 Abs. 2 SGB V) ausschließliche Angelegenheit der Kassenärztlichen Vereinigungen ist, im Rahmen von Plausibilitätsprüfungen die vertragsärztlichen Abrechnungen auf ihre Rechtmäßigkeit hin zu überprüfen.

Nach der einschlägigen Verfahrensordnung wird dem betroffenen Arzt zur Abgabe einer Stellungnahme Einsicht in den erstellten Prüfbericht und die vorliegenden Unterlagen gewährt. Sollte die Plausibilitätskommission nach Abgabe der ärztlichen Stellungnahme ein weiteres Gespräch für erforderlich halten, ist der betroffene Arzt zudem bei der Einladung zu dem Gespräch auf die Möglichkeit der Hinzuziehung eines Rechtsbeistandes bzw. eines Fachvertreters seines Vertrauens hinzuweisen. Die Bestimmungen der Verfahrensordnung sahen somit ausdrücklich sowohl das Recht des betroffenen Arztes auf Akteneinsicht als auch auf Hinzuziehung eines Rechtsbeistandes vor.

Dies führte zu folgender Bewertung: Auch in den von den Kassenärztlichen Vereinigungen durchzuführenden Plausibilitätsverfahren nach § 83 Abs. 2 SGB V stehen dem betroffenen Arzt die aus dem Grundrecht auf rechtliches Gehör resultierenden Verfahrensrechte auf Vertretung bzw. Akteneinsicht zu. Dies entspricht auch den Bestimmungen der §§ 13 Abs. 1 und 25 Abs. 1 SGB X, durch die das Grundrecht auf rechtliches Gehör auch im Sozialverwaltungsverfahren seinen ausdrücklichen Niederschlag gefunden hat und die im Zusammenhang mit der Durchführung von Plausibilitätsverfahren nach § 83 Abs. 2 SGB V entsprechend heranzuziehen sind. Aus datenschutzrechtlicher Sicht bestanden somit gegen die Gewährung der Akteneinsicht zugunsten des Arztbevollmächtigten keine Bedenken.

11.5 Disease-Management-Programme (DMP)

Die Komplexität unseres Gesundheitswesens findet ihren Ausdruck nicht nur in einer unübersichtichen Regelungsmaterie, sondern auch und gerade in seiner eigenständigen Terminologie (z. B. „Risikostrukturausgleich“, „diagnosebezogene Fallpauschale“), welche für den Laien kaum noch verständlich ist. Im Folgenden soll daher zunächst der Versuch unternommen werden, die sog. Disease-Management-Programme (DMP) zu erläutern, bevor die damit zusammenhängenden datenschutzrechtlichen Fragen dargestellt werden:

Unter dem Begriff DMP versteht man eine medizinische Versorgungsform, mit der die Behandlung chronischer Erkrankungen und die Prävention von Folgeschäden verbessert werden soll (Stichwort: „patientenbezogene Behandlungsoptimierung“). Konkret bedeutet dies, dass mit der Teilnahme sowohl für Ärzte als auch für Patienten bestimmte Mitwirkungspflichten (Bsp.: Teilnahme an Schulungen über Ernährungsfragen) begründet und seitens der Kassen überprüft werden.

Hintergrund ist der Umstand, dass in Deutschland mehr als zehn Millionen Menschen an chronischen Erkrankungen leiden, die einen Großteil der Kosten im Gesundheitswesen verursachen. Allein von Diabetes sind bundesweit zirka vier Millionen Menschen, in Rheinland-Pfalz ca. 200 000 Menschen, betroffen. Nach dem Gutachten des Sachverständigenrates für die konzertierte Aktion im Gesundheitswesen leidet das Gesundheitswesen in Deutschland unter einer Fehl-, Unter- oder Überversorgung von chronisch Kranken. Mit DMP soll daher eine bessere Versorgung chronisch Kranker erreicht werden. Eine Expertenkommission der Kassen, Krankenhäuser und der Ärzte hat vier Krankheiten als DMP-tauglich erklärt: Diabetes, Asthma, Brustkrebs und die koronare Herzkrankheit. Um finanzielle Anreize für die Krankenkassen zu schaffen, sich um diese vermeintlich „teuren Patienten“ besonders zu kümmern, erhalten diese durch eine Neuregelung im Risikostrukturausgleich mehr Geld für DMP.

Durch das Gesetz zur Reform des Risikostrukturausgleichs vom 10. Dezember 2001 wurde im SGB V (§ 137 f) eine Vorschrift zu strukturierten Behandlungsprogrammen bei chronischen Krankheiten aufgenommen und der Begriff DMP eingeführt. In Abkehr vom sonstigen Prinzip der gesetzlichen Krankenversicherung sollen den Krankenkassen im Rahmen von DMP auch patientenbezogene medizinische Daten bei der ambulanten Versorgung zur Kenntnis gelangen. Als zentrale datenschutzrelevante Vorschrift regelt § 137 f Abs. 3 SGB V jedoch, dass für die Versicherten die Teilnahme an DMP freiwillig ist und dass eine Einschreibung nur bei Vorliegen einer informierten schriftlichen Einwilligungserklärung der Betroffenen erfolgen darf.

Der Informationsfluss zwischen den an DMP beteiligten Stellen, insbesondere der Umfang der den Krankenkassen vorzulegenden Patientendokumentation, ist nach § 137 f SGB V in einer Rechtsverordnung zu regeln. Dies ist in der Vierten Verordnung zur Risikostrukturausgleichsverordnung (RSAV) geschehen. Mittlerweile ist bereits die Siebte RSAV in Kraft getreten.

Aus datenschutzrechtlicher Sicht sind die folgenden Regelungen der RSAV von besonderer Bedeutung:

- Nach § 28 f Abs. 2 Nr. 3 RSAV muss der Versicherte in jede einzelne Übermittlung gesondert schriftlich einwilligen.
- Die RSAV sieht vor, dass den Krankenkassen die Aufgabe der „Betreuung“ im Rahmen der DMP zukommt. Darüber hinaus findet jedoch auch eine (Erfolgs-)Kontrolle durch die Krankenkassen statt. In den Verträgen sollte daher eine möglichst konkrete Aufgabenbeschreibung der Krankenkassen vorgenommen werden, weil sich hierauf die Einwilligungserklärung des Versicherten, die Bestandteil der Verträge ist, zu beziehen hat.
- Die Krankenkassen erhalten für ihre Aufgabenerfüllung medizinische Daten der Versicherten. Welche dies konkret sind, ist in den Anlagen der RSAV geregelt. Nach § 28 f Abs. 2 RSAV besteht die Möglichkeit, dass die Krankenkassen mit den Kassenärztlichen Vereinigungen Verträge zum DMP abschließen. In diesen Fällen erhalten die Krankenkassen weniger personenbezogene Daten, insbesondere im Hinblick auf die Leistungserbringer. Kommen derartige Verträge nicht zustande, können die Krankenkassen mit den Vertragsärzten Einzelverträge abschließen. Bei dieser Verfahrensweise erhalten die Krankenkassen im Hinblick auf ihre Aufgaben bei DMP mehr personenbezogene Daten.
- Der Weg über die Kassenärztlichen Vereinigungen führt des Weiteren dazu, dass eine Arbeitsgemeinschaft zu gründen ist, welche insbesondere die Aufgabe der Pseudonymisierung und der Depseudonymisierung der Versichertendaten (z. B. für Zwecke der Qualitätssicherung und der Evaluation) zu übernehmen hat. Diese Aufgabe hat für den Fall, dass Verträge mit den Kassenärztlichen Vereinigungen nicht zustande kommen, die Krankenkasse zu übernehmen.
- Die Krankenkassen haben nach § 28 f Abs. 1 Nr. 2 RSAV sicherzustellen, dass nur bestimmte geschulte Mitarbeiter Zugang zu den DMP-Daten besitzen.

In Rheinland-Pfalz haben die vier Kassenärztlichen Vereinigungen mit den Betriebs-, Innungs- und Landwirtschaftskassen, der Bundesknappschaft sowie den Angestelltenkrankenkassen und Arbeiter-Ersatzkassen am 13. März 2003 den ersten DMP-Vertrag in Sachen Diabetes unterzeichnet. Die AOK hat einen Vertragsabschluss abgelehnt und beabsichtigt stattdessen, Einzelverträge mit den Vertragsärzten abzuschließen.

Die dem LfD vorgelegten Musterverträge waren inhaltlich stark an die Vorgaben des Bundesversicherungsamtes gebunden, so dass datenschutzrechtliche Änderungs- bzw. Ergänzungswünsche nur noch teilweise in Bezug auf die Einwilligungserklärung/Versicherteninformation möglich waren. Der LfD wird weitere Fragen, die insbesondere mit der Einschaltung einer Arbeitsgemeinschaft im Zusammenhang stehen, weiterhin kritisch begleiten und die gesetzeskonforme Umsetzung der o. g. Bestimmungen im Rahmen örtlicher Feststellungen regelmäßig überprüfen.

11.6 Arztgeheimnis und strafrechtliche Ermittlungen

Die Aufklärung von Tötungsdelikten zählt zweifelsohne zu den wichtigsten Aufgaben der Polizei. Damit sie diese Aufgabe wahrnehmen kann, sind ihr in der StPO umfangreiche Befugnisse eingeräumt worden. Diese umfassen selbstverständlich auch das Recht, die für die Aufklärung der Tat erforderlichen Informationen erheben zu dürfen. Fordert die Polizei im Rahmen ihrer Ermittlungstätigkeit jedoch Sozialdaten an, so beurteilt sich die Rechtmäßigkeit der Datenweitergabe durch den Sozialleistungsträger ausschließlich nach den Bestimmungen des Sozialgesetzbuches. Ein Umstand, der bei Delikten, bei denen ein entsprechender Ermittlungsdruck besteht, bisweilen übersehen wird. So auch in dem Fall, in dem die Polizei Ermittlungen im Zusammenhang mit dem Auffinden eines unbekannten toten Säuglings anstellte. In Abstimmung mit der Staatsanwaltschaft wurde eine Kassenärztliche Vereinigung gebeten, eine Liste der Frauen auszuhändigen, bei denen der errechnete Geburtstermin in dem Zeitraum des Auffindens des Säuglings lag. Die Kassenärztliche Vereinigung druckte daraufhin eine Liste mit Namen, Vornamen, Geburtsdatum, Anschrift und dem mutmaßlichen Entbindungstag der entsprechenden Patientinnen aus und übergab sie der Polizei. Diese schied aus dem Datenbestand diejenigen Mütter aus, deren Geburt amtlich registriert war. Die verbleibenden Frauen, bei denen keine Geburt festgestellt werden konnte, wurden im Rahmen einer schriftlichen Befragung aufgefordert, ärztliche Bescheinigungen über Abtreibung bzw. Totgeburten vorzulegen.

Einige der betroffenen Frauen wandten sich daraufhin Rat suchend an ihre jeweiligen Frauenärzte. Der Berufsverband der Frauenärzte, welcher auf diesem Weg von den Vorkommnissen unterrichtet wurde, wies in seinem Schreiben an die Kassenärztliche Vereinigung, die Staatsanwaltschaft sowie den LfD darauf hin, dass das Arzt-Patientengeheimnis durch die Vorgehensweise der Polizei in erheblichem Umfang ausgehöhlt würde. So könnten Frauen, welche einen legalen Abbruch vor ihrer Familie verheimlicht hätten, bei islamischer Herkunft in Lebensgefahr geraten, falls das Schreiben von Familienangehörigen gelesen würde.

Der Leitende Oberstaatsanwalt ließ nach Unterrichtung über den Vorgang die fragliche Ermittlungsaktion stoppen und die betreffenden Patientendaten vernichten. Diese Form der Schadensbegrenzung änderte jedoch nichts daran, dass die Datenerhebung der Ermittlungsbehörden und die Datenübermittlung der Kassenärztlichen Vereinigung mit den Vorschriften des Sozialgesetz-

buches nicht zu vereinbaren und damit rechtswidrig waren (vgl. § 35 Abs. 3 SGB I i. V. m. §§ 73 und 76 SGB X). Der LfD beanstandete den unzulässigen Informationsaustausch sowohl gegenüber der Kassenärztlichen Vereinigung als auch der Staatsanwaltschaft. Beide Institutionen haben in der Zwischenzeit durch interne Maßnahmen dafür Sorge getragen, dass solche Vorgänge künftig ausgeschlossen werden.

11.7 Anforderung medizinischer Unterlagen durch Krankenkassen bei Krankenhäusern

Im 18. Tätigkeitsbericht wurde unter Tz. 11.1.1 ausführlich über die Zulässigkeit der Anforderung medizinischer Unterlagen durch Krankenkassen bei Krankenhäusern berichtet. Anlass waren die aus Sicht des LfD unzutreffenden Urteile des Sozialgerichtes Speyer sowie des Landessozialgerichtes, welche im Berichtszeitraum vom Bundessozialgericht überprüft wurden. Das Bundessozialgericht schloss sich dabei der Rechtsauffassung des LfD vollinhaltlich an. Es stellte in seinem Urteil vom 23. Juli 2002 fest, dass Krankenkassen eine Einsichtnahme in Behandlungsunterlagen nicht aus eigenem Recht verlangen können, sondern insoweit auf ein Tätigwerden des MDK angewiesen sind. Der Praxis einiger Krankenkassen, die Begleichung der Krankenhausrechnung von der Vorlage von Patientendaten abhängig zu machen, ist damit ein Riegel vorgeschoben worden. Es bleibt zu hoffen, dass das Urteil des Bundessozialgerichts einen wesentlichen Beitrag dazu leisten kann, den lang andauernden Streit über diese wesentliche Frage innerhalb der gesetzlichen Krankenversicherung endlich beilegen zu können. Im Zuständigkeitsbereich des LfD ergibt sich mit dem Urteil des Bundessozialgerichtes jedoch kein konkreter Änderungsbedarf: Die der Kontrolle des LfD unterstehenden Krankenkassen hatten bereits in der Vergangenheit anerkannt, dass nach der Aufgabenverteilung in der gesetzlichen Krankenversicherung die Einsichtnahme in sensible medizinische Daten wie etwa Arzt-, Operations- und Krankenhausentlassungsberichte ausschließlich dem MDK vorbehalten ist.

11.8 Grundsicherungsgesetz

Für ältere und dauerhaft voll erwerbsgeminderte Menschen mit geringem Einkommen ist am 1. Januar 2003 ein neues Leistungsgesetz zur Sicherung des Lebensunterhaltes in Kraft getreten. Das GSiG sieht insoweit die Einführung einer von der Sozialhilfe unabhängigen Leistung vor, die die verschämte Altersarmut verhindern und voll erwerbsgeminderten Erwachsenen eine eigenständige materielle Absicherung ihres Lebensunterhaltes garantieren soll. Das entsprechende Ausführungsgesetz auf Landesebene legt als Träger der Grundsicherung die Landkreise und kreisfreien Städte fest, die diese Aufgabe jedoch an die Verbandsgemeinden delegieren können.

Mit dem In-Kraft-Treten des neuen Gesetzes wurden auch datenschutzrelevante Fragen aufgeworfen. So wollte eine Verbandsgemeinde beispielsweise wissen, ob die Sozialämter an die Grundsicherungsämter die Antragsdaten übermitteln dürfen oder ob zuvor das Einverständnis der Betroffenen einzuholen ist. Hierzu war festzustellen, dass nicht etwa die Verbandsgemeindeverwaltung insgesamt, sondern das Sozialamt der Verbandsgemeinde als verantwortliche Stelle im Sinne des § 67 Abs. 9 SGB X zu qualifizieren ist. Dies bedeutet, dass Informationsweitergaben des Sozialamtes an andere Stellen – auch innerhalb der Verbandsgemeindeverwaltung – rechtlich als Übermittlung von Sozialdaten zu qualifizieren sind. Diese sind nur nach Maßgabe des § 69 SGB X zulässig. Voraussetzung einer zulässigen Datenübermittlung ist hiernach stets die Erforderlichkeit der Informationsweitergabe. Im vorliegenden Fall waren die Grundsicherungsämter jedoch selbst in der Lage, die erforderlichen Daten bei den Betroffenen zu erheben. Dies entspricht im Übrigen auch dem sog. Ersterhebungsgrundsatz beim Betroffenen (vgl. § 67 a Abs. 2 SGB X).

Eine Datenerhebung beim Betroffenen hat im Übrigen den Vorteil, dass auch nur die Informationen erhoben werden, die für die Aufgabenerfüllung der Grundsicherungsämter tatsächlich benötigt werden. Aufgrund der unterschiedlichen Zielsetzungen des Sozialhilfeverfahrens einerseits und des Verfahrens über die bedarfsorientierte Grundsicherung andererseits besteht ansonsten die Gefahr nicht erforderlicher Datenweitergaben.

Da das Sozialgesetzbuch eine Übermittlung von Sozialdaten zur Verfahrenserleichterung („im Interesse des Betroffenen“) nicht kennt, konnten die entsprechenden Daten von dem Sozialamt nur dann zur Verfügung gestellt werden, wenn die Betroffenen zuvor eingewilligt hatten.

Auch die bundesweit zum Einsatz kommenden Formulare zur Durchführung des Grundsicherungsgesetzes wurden einer datenschutzrechtlichen Prüfung unterzogen. Als problematisch erwies sich dabei der Informationsaustausch zwischen Rentenversicherungsträger und Grundsicherungsträger, wenn eine volle Erwerbsminderung noch nicht festgestellt worden ist. Die Beantwortung der Frage, ob der Grundsicherungsträger seinerseits überhaupt personenbezogene Daten erheben darf und bei welcher Stelle die Unterlagen dauerhaft aufzubewahren sind, hängt nämlich davon ab, welche Zuständigkeitsverteilung zwischen Grundsicherungs- und Rentenversicherungsträger besteht und ob der Entscheidung des Rentenversicherungsträgers Bindungswirkung für das Grundsicherungsamt zukommt. Die Fragen werden derzeit vom BfD mit dem Verband der Rentenversicherungsträger geklärt, um eine einheitliche Verfahrensweise zu erreichen.

12. Datenschutz im Ausländerwesen

12.1 Überprüfung von Speicherungen im Schengener Informationssystem

In seinem 17. Tb. hatte der LfD von vermehrt vorgelegten Prüfungsersuchen des Personenkreises, der im SIS zur Einreiseverweigerung ausgeschrieben war, berichtet. Die Überprüfungen im aktuellen Berichtszeitraum haben – abweichend von den im 17. Tb. dargelegten Feststellungen – ergeben, dass in der überwiegenden Anzahl der geprüften Ausschreibungen die Ausschreibungsfristen zu lang gewählt worden waren. Der LfD sah in den nachstehend aufgeführten Prüffällen Anlass, die Löschung der Ausschreibung im SIS zu empfehlen:

Rechtsgrundlage für Ausschreibungen zum Zweck der Einreiseverweigerung bildet Art. 96 SDÜ i. V. m. Ziffer 2.2.1.3 der einschlägigen Allgemeinen Anwendungshinweise zum Schengener Durchführungsübereinkommen. Die Vorschrift kann dann nicht herangezogen werden, wenn die Ausschreibung lediglich den Zweck der Aufenthaltsermittlung untergetauchter abgelehnter Asylbewerber verfolgt. Der Empfehlung des LfD, die unzulässigen Ausschreibungen im SIS sowie zur Festnahme in INPOL zu löschen und zur Aufenthaltsermittlung in INPOL oder im AZR auszuschreiben, kamen die Ausländerbehörden regelmäßig nach.

Gemäß Ziffer 2.2.2.1 der vorgenannten Allgemeinen Anwendungshinweise beträgt die Ausschreibungsfrist bei Abschiebungen nach §§ 49 ff. AuslG – unbeschadet einer Verlängerung – drei Jahre. Hält es die Ausländerbehörde für erforderlich, die Ausschreibung einmalig um weitere drei Jahre zu verlängern, ist dagegen grundsätzlich nichts einzuwenden. Eine Löschung hält der LfD dann für geboten, wenn die für eine darüber hinausgehende weitere Verlängerung erforderlichen neuen Anhaltspunkte oder besonderen Gründe in den jeweiligen Prüffällen nicht vorliegen. Die Ausländerbehörden waren den Empfehlungen des LfD auch in diesen Fällen gefolgt.

12.2 Darf das Ausländeramt einem getrennt lebenden noch nicht geschiedenen Ehemann einer Ausländerin Auskunft über den Aufenthaltsort seiner Gattin geben?

Auf entsprechende Fragen von Ausländerämtern hat der LfD wie folgt geantwortet:

Die noch bestehende oder ehemalige Ehe allein stellt in keinem Fall für sich genommen einen Rechtsgrund für eine Auskunftserteilung dar.

Die Datenverarbeitungsregelungen des Ausländergesetzes (§§ 75 bis 80 AuslG) betreffen diese Fälle nicht. Es ist deshalb auf die allgemeinen datenschutzgesetzlichen Regelungen über Datenübermittlungen an Private in § 16 Abs. 1 LDSG zurückzugreifen.

Folgende Übermittlungsalternativen kommen danach in Betracht:

Gemäß § 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 1 Nr. 2 LDSG
ist eine Übermittlung zulässig, wenn die Betroffenen eingewilligt haben; dies kommt in den geschilderten Fällen, in denen Streit zwischen den ehemaligen oder noch verbundenen Ehegatten besteht, offensichtlich nicht in Betracht.

Gemäß § 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 1 Nr. 4 LDSG,
wenn die Übermittlung zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist; dies ist in Fällen der vorliegenden Art, in denen es allein um Interessen der Anfrager geht, ebenfalls regelmäßig ausgeschlossen.

Gemäß § 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 1 Nr. 5 LDSG,
wenn dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist; ein solcher Fall wäre vorstellbar; es müssten aber entsprechende Gesichtspunkte seitens des Anfragenden nachgewiesen werden.

Gemäß § 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 1 Nr. 9 LDSG,
wenn die Daten allgemein zugänglich sind und wenn keine Anhaltspunkte vorliegen, dass der Datenübermittlung überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen; dies kommt in Betracht, wenn die Adresse tatsächlich z. B. im Telefonbuch vermerkt ist und nicht von einer streitigen Auseinandersetzung zwischen den Beteiligten auszugehen ist; im Zweifel empfiehlt sich vor einer Datenübermittlung eine Anfrage bei der betroffenen Person, um deren Daten es geht.

Nach § 16 Abs. 1 Nr. 3 LDSG wird eine Datenübermittlung auch durch ein rechtliches Interesse gerechtfertigt, wenn keine überwiegenden schutzwürdigen Belange des Betroffenen ersichtlich sind. Der Begriff des rechtlichen Interesses ist vom „berechtigten Interesse“ deutlich zu unterscheiden. Damit ist nicht jedes von der Rechtsordnung bloß anerkannte Interesse gemeint, dessen Verwirklichung Ausfluss der allgemeinen Handlungsfreiheit ist. Hiermit sind vielmehr Interessen bezeichnet, die mit Hilfe der Rechtsordnung durchgesetzt und vollstreckt werden können. In erster Linie handelt es sich hier also um Rechtsansprüche gegen andere Private oder gegen öffentliche Stellen, zu deren Realisierung Informationen benötigt werden. Auch hier ist eine detaillierte plausible Darlegung durch den Antragsteller gefordert und auch hier ist im Falle eines Streits zwischen den Beteiligten grundsätzlich von einer Übermittlung abzusehen. Auch hier empfiehlt sich im Zweifel eine Anfrage bei der betroffenen Person, um deren Daten es geht.

Nach § 16 Abs. 1 Nr. 4 LDSG schließlich wird eine Datenübermittlung auch durch ein berechtigtes Interesse gerechtfertigt, wenn der Betroffene nach Unterrichtung über die beabsichtigte Datenübermittlung keinen Widerspruch erhoben hat. Auch dies käme in Betracht; es wäre aber sicherzustellen, dass der oder die Betroffene tatsächlich eine entsprechende Unterrichtung in einer ihm oder ihr verständlichen Sprache erhalten hat. Eine Verpflichtung der Ausländerbehörde, dieses Verfahren einzuleiten und die Datenübermittlung durch Übersenden einer solchen Unterrichtung vorzubereiten, besteht grundsätzlich nicht. Insofern hat die datenübermittelnde Stelle ein Ermessen. Der Auskunftbegehrende müsste außerordentliche Umstände geltend machen, um eine solche Pflicht der Behörde begründen zu können. Im Allgemeinen kann sich die Behörde auf die mit diesem Verfahren einhergehende zusätzliche Arbeitsbelastung oder auch auf eine entsprechend bestehende generelle Übung der Ablehnung dieses Verfahrens berufen, um dem Anliegen der Auskunftbegehrenden entgegenzutreten.

12.3 Besucherbücher in Asylbewerberunterkünften

Aufgrund der Anfrage eines anderen Landesbeauftragten für den Datenschutz hat der LfD geklärt, ob in rheinland-pfälzischen Asylbewerberunterkünften Besucherbücher geführt werden und welche konkreten Bedingungen dafür jeweils gelten.

Es hat sich ergeben, dass dies in den Landesunterkünften aus Gründen der Sicherheit und Ordnung (unter dem Gesichtspunkt der Wahrung des Hausrechts) zulässigerweise erfolgt.

Es hat sich allerdings auch ergeben, dass die entsprechenden Bücher mit den Eintragungen über alle Besuche fünf Jahre aufbewahrt werden.

Aus datenschutzrechtlicher Sicht erscheint eine Aufbewahrungszeit von fünf Jahren für die Informationen über Besuche in einer Asylbewerberunterkunft als erheblich zu lang. In diesem Zusammenhang war auch die Sach- und Rechtslage in anderen Bundesländern zu berücksichtigen: In Nordrhein-Westfalen wird die Führung solcher Besucherbücher insgesamt für rechtswidrig gehalten, sie unterbleibt. In Thüringen wird jedenfalls die kurzfristige Löschung der Daten verlangt. Vor diesem Hintergrund hat der LfD eine kurze am Erfordernis der Datenspeicherung orientierte Löschfrist gefordert.

12.4 Lichtbildanforderungen durch Bußgeldbehörden an die Aufnahmeeinrichtungen

Auf die Frage des zuständigen Ressorts, wie der LfD die Frage beurteile, ob und unter welchen Voraussetzungen von den Aufnahmeeinrichtungen für Asylbewerber bzw. sonstige Flüchtlinge, deren Lichtbilder an die Bußgeldbehörden übermittelt werden dürften, wurde folgende Stellungnahme abgegeben:

Das Asylverfahrensgesetz enthält in § 8 Abs. 3 Satz 1 für Asylbewerber die ausdrückliche Regelung, dass deren Daten (worunter auch Lichtbilder fallen) zur Verfolgung von Ordnungswidrigkeiten auf Ersuchen den damit betrauten öffentlichen Stellen, soweit es zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist, übermittelt werden dürfen.

Das Ausländergesetz enthält weder spezielle vorrangige Regelungen für die Datenübermittlung an Bußgeldbehörden zum Zweck der Durchführung von Ordnungswidrigkeitenverfahren, noch ist dem Ausländergesetz eine besondere Zweckbindungsregelung für Daten zu entnehmen, die von den Ausländerbehörden gespeichert werden.

Für solche Daten der Ausländerbehörden, die nicht dem Asylverfahrensgesetz unterliegen, gelten also im vorliegenden Zusammenhang die Regelungen der §§ 46 Abs. 1 und 2 OwiG i. V. m. § 161 StPO unmittelbar. Danach ist die Bußgeldbehörde befugt, von allen Behörden Auskunft zu verlangen. Die Behörden sind verpflichtet, dem Ersuchen zu genügen.

In jedem Fall gilt aber das Verhältnismäßigkeitsprinzip und der damit verbundene Erforderlichkeitsgrundsatz. Dem wird bei Anwendung der Grundsätze Rechnung getragen, die in einem besonderen Rundschreiben für entsprechende Lichtbildanforderungen aus dem Pass- und Personalausweisregister festgelegt sind.

Bei Vollzugshilfeersuchen anderer Bundesländer haben die ersuchenden Stellen selbst vor Absendung des Ersuchens den Verhältnismäßigkeitsgrundsatz in eigener Verantwortung zu prüfen. Die ersuchten rheinland-pfälzischen Dienststellen haben dann, wenn zu weitergehenden Prüfungen kein Anlass ersichtlich ist, nur zu beurteilen, ob das Ersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt (§ 14 Abs. 2 LDSG).

13. Datenschutz in der Finanzverwaltung

13.1 Gesetzliche Änderungen

13.1.1 Neues Abrufverfahren bei den Kreditinstituten

Im Rahmen des 4. Finanzmarktförderungsgesetzes wurde auch das Kreditwirtschaftsgesetz novelliert. Dieses sieht nunmehr vor, dass die Kreditinstitute eine Datei führen, in der die Nummer eines Kontos, das der Verpflichtung zur Legitimationsprüfung im Sinne der Abgabenordnung unterliegt, sowie Name und Geburtsdatum des Inhabers und eines Verfügungsberechtigten gespeichert werden. Aus dieser Datei haben die Banken der Bundesanstalt für Finanzdienstleistungsaufsicht unter bestimmten Voraussetzungen Informationen zu übermitteln. Darin haben die Datenschutzbeauftragten des Bundes und der Länder einen neuen Eingriff in die Vertraulichkeit der Bankbeziehungen gesehen und daher auf ihrer 63. Konferenz im März 2002 eine Entschließung gefasst (s. Anlage 10). Darin fordern sie insbesondere, dass die Bankkunden von ihren Kreditinstituten über die Datenspeicherungen informiert werden. Wie die Praxis zeigt, erfolgt gerade diese Information nicht ausreichend. So sollte ein Petent seiner Sparkasse den Personalausweis vorlegen, da man aufgrund „gesetzlicher Bestimmungen“ zur Legitimationsprüfung und zur Datenspeicherung verpflichtet sei. Dem Petenten war völlig unklar, wieso er nach vielen Jahren, in denen er bereits Kunde der Sparkasse war, plötzlich seinen Personalausweis vorlegen sollte. Die Sparkasse hat auf Empfehlung des LfD nunmehr die Rechtsgrundlagen ausdrücklich benannt.

13.1.2 Freistellung vom Steuerabzug bei Bauleistungen

Seit 1. Januar 2002 haben bestimmte Auftraggeber von Bauleistungen im Inland einen Steuerabzug in Höhe von 15 % der Gegenleistung für Rechnung des die Bauleistung erbringenden Unternehmens vorzunehmen, wenn nicht eine vom zuständigen Finanzamt ausgestellte Freistellungsbescheinigung vorliegt. Die in der Bescheinigung anzugebenden Daten sind in § 48 b EStG abschließend aufgezählt. Obwohl dort das Geburtsdatum nicht genannt ist, wurde von den Finanzämtern dieses Datum in die Bescheinigungen aufgenommen. Das Ministerium der Finanzen wurde durch den LfD darauf hingewiesen, dass eine Freistellungsbescheinigung in dieser Form keine gesetzliche Grundlage hat.

Weiterhin ist vorgesehen, dass das Bundesamt für Finanzen dem Leistungsempfänger im Wege einer elektronischen Abfrage Auskunft über die beim Bundesamt gespeicherten Freistellungsbescheinigungen erteilt. Der Antragsteller stimmt mit dem Antrag auf Erteilung einer Freistellungsbescheinigung zu, dass seine Daten beim Bundesamt für Finanzen gespeichert werden und darüber Auskunft an die Leistungsempfänger erteilt wird. Im überarbeiteten Merkblatt zum Steuerabzug bei Bauleistungen wird nunmehr zwar auf die Möglichkeit einer Internet-Anfrage beim Bundesamt für Finanzen hingewiesen, weitere Informationen – das Verfahren betreffend – sind jedoch nicht enthalten. Aufgrund der Hinweise des LfD hätte die Überarbeitung des Merkblatts durchaus datenschutzfreundlicher ausfallen können.

13.1.3 Angabe der Steuernummer auf Rechnungen und das Steuergeheimnis

Ab 1. Juli 2002 sind alle Unternehmer verpflichtet, auf Rechnungen ihre Steuernummer anzugeben. Das sieht der durch das Steuerverkürzungsbekämpfungsgesetz eingeführte § 14 Abs. 1 a UStG vor – eine Regelung, die von den Datenschutzbeauftragten durchaus kritisch betrachtet wird, da sie das Recht auf informationelle Selbstbestimmung einschränkt. Sie ist jedoch als verfassungskonform zu bewerten.

Mit der Neuerung geht die Befürchtung einher, dass sich Unberechtigte durch missbräuchliche Verwendung der Steuernummer – insbesondere telefonisch – Informationen über Steuerpflichtige verschaffen können. Es ist jedoch davon auszugehen, dass die Finanzverwaltung hinsichtlich der Auskunftserteilung bei Nennung einer Steuernummer am Telefon hinreichend sensibilisiert ist und das Steuergeheimnis wahrt. So reicht die Kenntnis der Steuernummer als Legitimation für die Weitergabe von Informationen keinesfalls aus. Vielmehr wurden zusätzliche Kriterien für die Identitätsprüfung des Anrufers herangezogen, wie z. B. persönliche Bekanntheit des Steuerpflichtigen oder Detailkenntnisse aus dem angesprochenen Vorgang. In Zweifelsfällen erfolgt ein Rückruf durch die Mitarbeiter des Finanzamtes bzw. es wird eine schriftliche Antwort erteilt. Auf diese Anforderungen hat die OFD Koblenz die Finanzämter mit Rundverfügungen erneut hingewiesen. Diese Handhabung fand der LfD bei örtlichen Feststellungen in der Finanzverwaltung bestätigt.

13.2 Einzelfragen

13.2.1 Informationsweitergabe aus einem kommunalen Gebührenverfahren

Eine Kreisverwaltung hatte sich in folgender Angelegenheit an den LfD gewandt:

Bei der Bearbeitung von Abfallgebührenverfahren erhielten die zuständigen Mitarbeiter hin und wieder Informationen, aus denen zu schließen wäre, dass die betroffenen Bürger von anderen Behörden Leistungen in Anspruch nehmen, die ihnen tatsächlich nicht zustünden, aber durch falsche Angaben gegenüber diesen Behörden erschlichen würden. Hierzu wurden drei Beispielsfälle geschildert:

– Ein Bürger sollte für sich und das bei ihm gemeldete Kind Abfallgebühren entrichten. Daraufhin trägt er gegenüber der Kreisverwaltung vor, das Kind wohne gar nicht bei ihm, sondern sei nur dort gemeldet, damit er das Kindergeld erhalte. Tatsächlich lebe das Kind bei der Mutter in England.

– Ein Lehrer übe seine Tätigkeit in Warschau aus, habe aber seinen Hauptwohnsitz aus steuerlichen Gründen im Kreis gemeldet. Da er dort aber tatsächlich nicht wohne, wolle er auch keine Müllgebühr bezahlen.

– Ein Gewerbetreibender, der zur Abfallentsorgung veranlagt werden soll, behauptet, keinerlei Betriebsräume zu haben und beim Finanzamt auch keine Betriebsräume steuerlich geltend zu machen.

Bei der datenschutzrechtlichen Beurteilung war von folgenden rechtlichen Erwägungen auszugehen:

Die in einem Abfallgebührenverfahren gewonnenen Erkenntnisse unterliegen dem Steuergeheimnis. Eine Übermittlung ist daher nur unter den Voraussetzungen von § 30 Abs. 4 AO zulässig.

Eine Offenbarungsbefugnis konnte sich allenfalls aus § 30 Abs. 4 Nr. 1 AO ergeben, wenn die Offenbarung der Durchführung eines Verwaltungsverfahrens in Steuersachen dient. Denn die Informationen, die die Kreisverwaltung aus den Beschwerden über die Gebührenfestsetzung erhielt, wären zumindest in den beiden letztgenannten Fällen geeignet gewesen, ein steuerliches Verfahren gegen die Betroffenen einzuleiten.

Hierbei war jedoch zu bedenken, dass die Offenbarungsbefugnisse des § 30 Abs. 4 Nr. 1 AO auf eine Übermittlung innerhalb des Steuergeheimnisträgers abzielen. Eine Weiterleitung an eine andere außerhalb der Finanzverwaltung stehende Verwaltung ist nicht vorgesehen. Für kommunale Gebietskörperschaften, die kommunale Abgaben erheben, gilt diese Vorschrift der AO entsprechend. Folglich war davon auszugehen, dass auch die kommunale Gebietskörperschaft als einheitlicher Steuergeheimnisträger anzusehen ist und die Finanzverwaltung als außerhalb dieses Kreises stehende Behörde betrachtet werden muss. Demnach war eine Datenübermittlung durch die Kreisverwaltung an die Finanzbehörden nicht zulässig. Diese Auffassung wurde vom Ministerium des Innern und für Sport geteilt.

13.2.2 Daten von Berufskraftfahrern mit ausländischem Arbeitgeber und Wohnsitz in Deutschland

Die OFD Koblenz bat die ADD um Übermittlung von Namen der Berufskraftfahrer, die bei einem ausländischen Arbeitgeber beschäftigt waren, ihren Wohnsitz aber in Deutschland hatten. Diese waren in Deutschland zur Einkommensteuer verpflichtet. Aufgrund der Angaben wollte man überprüfen, ob diese Arbeitnehmer alle ordnungsgemäß besteuert würden. Dazu musste die Finanzverwaltung zunächst die Namen der Betroffenen ermitteln.

Der ADD lagen die Daten der entsprechenden Kraftfahrer vor, die eine Ordnungswidrigkeit in Ausübung ihrer Tätigkeit begangen hatten. Folglich hätten die Namen dieser Fahrer an die OFD übermittelt werden können. Gegen eine entsprechende Informationsweitergabe bestanden jedoch datenschutzrechtliche Bedenken: Als Rechtsgrundlage für eine Übermittlung kam § 93 Abs. 1 AO in Betracht. Danach haben u. a. auch Behörden der Finanzverwaltung die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlichen Auskünfte zu erteilen. Die Namen und Adressen der Betroffenen waren durchaus Informationen im Sinne dieser Vorschrift. Jedoch wäre mit diesen Daten auch stets die Information übermittelt worden, dass der Betroffene im Rahmen eines Ordnungswidrigkeitenverfahrens aufgefallen war und mit großer Wahrscheinlichkeit auch einen Bußgeldtatbestand erfüllt hatte. Diese Information war für das Besteuerungsverfahren nicht erforderlich. Da sie sich aber von den anderen erforderlichen Informationen nicht trennen ließ, war die gesamte Übermittlung nicht zulässig.

13.2.3 Auf den Hund gekommen I

Ein Petent war Halter eines Hundes und von der Hundesteuer befreit, da das Steueramt der Verbandsgemeinde aufgrund der Eintragung des Merkmals „Hilflos“ im vorgelegten Schwerbehindertenausweis davon ausging, dass das Halten des Hundes für den Petenten unentbehrlich war. Nunmehr erhielt die Verbandsgemeinde vom Bürgermeister der Ortsgemeinde Hinweise zum Hund des Petenten, die das Steueramt zum Anlass nahm, die damals erteilte Steuerbefreiung erneut zu überprüfen. Der Petent sollte Angaben machen, die eine Überprüfung ermöglichten, ob die Voraussetzungen für die Hundesteuerbefreiung vorlagen. Dabei war zu klären, ob das Halten des Hundes als Begleit- und Schutzhund für den Petenten unentbehrlich und ob der Hund als Begleit- und Schutzhund geeignet war.

Die Mitteilungen des Ortsbürgermeisters über den Hund an die Verbandsgemeinde waren datenschutzrechtlich nicht zu beanstanden. Er hatte lediglich Tatsachen mitgeteilt, die ohnehin offensichtlich waren. Es war wohl ortsbekannt, dass der Petent einen Hund besitzt. Zudem ist die Ortsgemeinde Gläubigerin der Hundesteuerschuld. Der Ortsbürgermeister als Vertreter der Ortsgemeinde konnte daher ohnehin eine Überprüfung der ordnungsgemäßen Hundesteuerzahlung veranlassen.

Als das Steueramt auf den Hund aufmerksam wurde, war es berechtigt zu überprüfen, ob Hundesteuer entrichtet wird. Aufgrund der Feststellung, dass und unter welchen Umständen für den Hund damals eine Steuerbefreiung bewilligt wurde, hielt das Steueramt eine Überprüfung der Angelegenheit für erforderlich. Im Rahmen dieses steuerlichen Verfahrens war der Petent zur Auskunft

verpflichtet. Er musste die Informationen weitergeben, die zur Beurteilung der Unentbehrlichkeit des Hundes erforderlich waren. Die Entscheidung des Steueramtes, dass das Merkmal „Hilflos“ im Schwerbehindertenausweis zum Nachweis nicht ausreichend sei, war nicht zu beanstanden. Die an den Petenten gestellten Fragen waren geeignet und auch verhältnismäßig, um die Unentbehrlichkeit zu beurteilen. Im Verhalten der Verbandsgemeinde war daher kein Verstoß gegen datenschutzrechtliche Vorschriften zu sehen.

In diesem Zusammenhang prüfte das Steueramt, ob die Führerscheinstelle von den vorgebrachten Krankheitssymptomen des Petenten in Kenntnis zu setzen war, da evtl. Fahruntüchtigkeit bestand. Auch eine solche Datenübermittlung war datenschutzrechtlich nicht zu beanstanden. Eine Offenbarung der in einem Steuerverfahren erlangten Kenntnisse ist dann zulässig, wenn hierfür ein zwingendes öffentliches Interesse besteht. Ein solches liegt vor, wenn im Fall des Unterbleibens der Mitteilung Gefahr bestünde, dass schwere Nachteile für das allgemeine Wohl eintreten. Hätte sich ergeben, dass der Petent trotz seiner aufgezählten Beschwerden (insbesondere Schwindelanfälle und Koma) ein Fahrzeug geführt hätte, konnte er dadurch andere gefährden. Es hätte eine konkrete Gefahr für die öffentliche Sicherheit bestanden, die eine Überprüfung seiner Fahrtauglichkeit gebot. Nur durch eine solche Datenübermittlung hätten schwere Nachteile für das Allgemeinwohl, nämlich eine konkrete Gefährdung des Straßenverkehrs, abgewendet werden können.

13.2.4 Auf den Hund gekommen II

Eine Petentin erhielt vom Steueramt ihrer Verbandsgemeinde einen Hundesteueränderungsbescheid. Danach sollte sie eine höhere Hundesteuer bezahlen als bisher, da sie einen gefährlichen Hund hielt. Die Petentin hatte aber nur gegenüber dem Ordnungsamt, nicht aber gegenüber dem Steueramt Angaben zur Hunderasse gemacht. Das Steueramt der Verbandsgemeinde hatte zwar zweimal um Mitteilung der Hunderasse gebeten, dieser Aufforderung war die Petentin aber nicht nachgekommen. Es stellte sich heraus, dass der Ehemann der Petentin in einem Schreiben in anderer Angelegenheit an den Bürgermeister und die Stadtratsmitglieder die Rasse des Hundes erwähnte. Die Petentin wandte sich dagegen, dass Informationen von dritter Seite dazu verwendet wurden, die Hundesteuer für sie neu festzusetzen.

Das Vorgehen der Verbandsgemeinde war jedoch nicht zu beanstanden. Nach § 93 AO haben die Beteiligten und andere Personen die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlichen Auskünfte zu erteilen. Andere Personen als die Beteiligten sollen erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch den Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Diese Vorschrift ist nach Kommunalabgabengesetz auch auf kommunale Steuern wie die Hundesteuer anwendbar. Die Petentin wurde zweimal aufgefordert, einen Fragebogen zur Erfassung der Hunderasse auszufüllen. Die Hunderasse war eine für die Besteuerung erforderliche Information. Da man diese Auskunft von ihr trotz zweimaliger Anfragen nicht erhalten hatte, durfte die Verbandsgemeinde andere Informationsquellen heranziehen. Zu diesem Zweck durfte sie nicht nur das Schreiben des Ehemannes verwenden, sondern hätte diesen auch direkt befragen können.

14. Wirtschaft und Verkehr

14.1 Änderung der Gewerbeordnung

Das Dritte Gesetz zur Änderung der Gewerbeordnung (BGBl. I S. 3412) ist am 1. Januar 2003 in Kraft getreten. Datenschutzrechtlich bedeutsam sind insbesondere die Neuregelungen in den §§ 11 und 14 GewO. In der Gesetzesbegründung wird darauf hingewiesen, dass eine Gewerbebehörde, die bei der Erfüllung ihrer Aufgaben erfährt, dass ein Berufskraftfahrer nicht mehr fahrtauglich ist, die Fahrerlaubnisbehörde nach der bisherigen Rechtslage darüber nicht unterrichten durfte. Aufgrund der Änderung des § 11 Abs. 6 GewO ist nunmehr eine Rechtsgrundlage für die Information der Fahrerlaubnisbehörde gegeben.

Gemäß dem neu eingefügten § 14 Abs. 1 a GewO teilen die Finanzbehörden den zuständigen Behörden den Namen und die Anschrift der Gewerbetreibenden mit, die ihr Gewerbe beim Finanzamt abgemeldet haben. In der Gesetzesbegründung wird hierzu dargelegt, dass Gewerbetreibende in vielen Fällen die Beendigung ihrer selbständigen Tätigkeit lediglich bei dem für sie zuständigen Finanzamt abmelden, um künftige steuerliche Verpflichtungen, insbesondere Steuererklärungspflichten zu vermeiden. Allerdings würden sie dem Gebot des § 14 GewO zur Abmeldung bei der Gewerbebehörde häufig nicht nachkommen, weshalb die neue Regelung erforderlich sei.

14.2 Bundeseinheitliche Wirtschaftsnummer in der Erprobung

Im Mai 2002 wurde das Gesetz zur Vorbereitung einer bundeseinheitlichen Wirtschaftsnummer verkündet (BGBl. I S. 1644). Im Rahmen der Initiative der Bundesregierung „Abbau von Bürokratie“ soll mit diesem „Wirtschaftsnummererprobungsgesetz“ die Kommunikation zwischen Behörden und Unternehmen verbessert werden. So gibt es im Wirtschaftsleben beispielsweise in den verschiedenen Behörden, Kammern, bei den Sozialversicherungsträgern sowie bei den jeweiligen Registern eine große Nummern- und Aktenzeichenvielfalt. Zukünftig sollen alle wirtschaftlich Tätigen eine Nummer erhalten, die für alle Behörden verbindlich ist, um die Unzulänglichkeit des bisherigen Nummerierungssystems zu beseitigen. Die Erprobung wird bis Ende 2003 in Bayern durchgeführt. Die Bundesregierung möchte dann im Jahr 2005 eine bundeseinheitliche Wirtschaftsnummer für Unternehmen, Betriebe und sonstige wirtschaftlich Tätige einführen. Mit dem Gesetz soll die Vergabe und Pflege der Wirtschaftsnummer und des

damit verbundenen Stammdatensatzes vorab getestet werden. Dieser Stammdatensatz enthält die Felder Name, Vorname, Firma, Anschrift, Rechtsform, Handels-, Genossenschafts- oder Vereinsregistereintragung, Wirtschaftszweig, Zeitpunkt der Aufnahme der Tätigkeit und Zeitpunkt der Beendigung der Tätigkeit. Zentrale Vergabe- und Speicherstelle ist die Bundesanstalt für Arbeit. Am Erprobungsprojekt beteiligt sind die betroffenen Finanzämter, die Gewerbebehörden, das Bayerische Landesamt für Statistik sowie die Industrie- und Handelskammern, die Handwerkskammern, die Kammern der freien Berufe, die Landwirtschaftskammer, die Berufsgenossenschaften und die Sozialversicherungsträger. Die betroffenen Firmen werden verpflichtet, die Nummer im Kontakt mit den genannten Stellen zu nutzen.

Betroffen von diesem Verfahren sind alle juristischen und natürlichen Personen, die im Wirtschaftsleben nicht abhängig arbeiten. Dies sind auch sämtliche Kleinbetriebe, etwa Freiberufler, Kleingewerbetreibende sowie alle privaten Haushalte, welche eine Haushaltshilfe beschäftigen. In diesem Zusammenhang ist es aus der Sicht des Datenschutzes natürlich besonders wichtig, der Gefahr zu begegnen, dass sich die geplante bundeseinheitliche Wirtschaftsnummer zu einem allgemeinen Personenkennzeichen entwickelt. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil zum Ausdruck gebracht, dass die Verknüpfung der bei den verschiedenen Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbestände durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal und damit die Erstellung von Persönlichkeitsprofilen der Bürger durch die Zusammenführung von Daten aus verschiedenen Lebensbereichen unzulässig wäre. Die bundesweite und behördenübergreifende Wirtschaftsnummer erfasst die betroffenen natürlichen Personen allerdings nur in einem ganz bestimmten Lebensbereich, nämlich ihrer wirtschaftlichen Betätigung. Daher hat die Wirtschaftsnummer – bei Beachtung der erwähnten verfassungsgerichtlichen Vorgaben – nach dem gegenwärtigen Verfahrensstand nicht die Eigenschaft eines unzulässigen Personenkennzeichens.

Datenschutzrechtlich bedenklich ist allerdings das Einbeziehen jener (natürlichen) Personen, die eine Haushaltshilfe beschäftigen, in den Kreis der Beteiligten, die eine einheitliche Wirtschaftsnummer erhalten. Als Beispiel seien hier berufstätige Ehepaare oder Rentner angeführt, die mit der Beschäftigung einer Haushaltshilfe zwar eine Dienstleistung in Anspruch nehmen, die jedoch ganz eindeutig der Privatsphäre zuzuordnen ist. Für diesen Personenkreis – der nicht im herkömmlichen Sinn wirtschaftlich tätig wird – ist daher die Vergabe einer Wirtschaftsnummer abzulehnen.

Die Erprobungsphase wird insbesondere seitens des BfD begleitet mit dem Ziel, datenschutzrechtliche Mängel des Projekts rechtzeitig zu erkennen und möglichst zu beheben. Erst nach der Auswertung der Erprobungsphase ist absehbar, ob die Einführung einer bundeseinheitlichen Wirtschaftsnummer in rechtlich abgesicherten Bahnen verlaufen kann. Über die weitere Entwicklung wird der LfD berichten.

14.3 Übernahme eines IHK-Datenbestandes durch Privatunternehmen unzulässig

Der LfD hatte sich mit der Anfrage einer IHK zu befassen, wie das Begehren einer Privatfirma – die Wirtschaftsinformationen vermarktet – auf Übernahme der bei dem Rechenzentrum der Industrie- und Handelskammern geführten Unternehmensdaten datenschutzrechtlich einzuordnen ist.

Diesbezüglich war zunächst darauf hinzuweisen, dass die Kammern als juristische Personen des öffentlichen Rechts, die der Aufsicht eines Landes unterstehen, den Datenschutzgesetzen dieses Landes unterliegen. Schutzgegenstand sind nur personenbezogene Daten, die als Einzelangaben über persönliche oder sachliche Verhältnisse von natürlichen Personen definiert werden. Personenbezogen sind also nur die Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Juristische Personen genießen nicht den Schutz der Datenschutzgesetze.

Die hier einschlägigen bereichsspezifischen Bestimmungen zum Datenschutz sind in § 9 IHK-Gesetz niedergelegt. Dort sind in Abs. 4 die Zulässigkeit und Voraussetzung der Übermittlung von Daten durch die Kammern an nicht öffentliche Stellen geregelt. Hier ist zu unterscheiden zwischen Daten, zu deren Weitergabe die Kammern berechtigt sind, soweit es dem Wirtschaftsverkehr dient, 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 in die Öffentlichkeit (z. B. bei der Werbung) begibt.

Im vorliegenden Fall war jedoch zu beachten, dass nicht lediglich eine Datenübermittlung im Raum stand, sondern die Übernahme des Datenbestandes durch ein Privatunternehmen. Diese beabsichtigte Form der Datenübermittlung bedeutet eine vom Gesetz nicht gedeckte Qualitätsänderung. Wenn der Gesetzgeber eine solche Verfahrensweise für zulässig halten würde, hätte er sicherlich entsprechende Regelungen zur Übernahme von Datenbeständen erlassen.

Nach allem hielt der LfD die beabsichtigte Datenübernahme insgesamt für unzulässig – auch hinsichtlich jener Daten, die nach § 9 Abs. 4 Satz 1 IHK-Gesetz vom Widerspruchsrecht ausgenommen sind.

Diese Sichtweise ist mit dem zuständigen Referat des Wirtschaftsministeriums abgestimmt.

14.4 Beitreibung von IHK-Beitragsrückständen durch ein Inkasso-Unternehmen?

An den LfD wurde die Frage herangetragen, wie die Beitreibung von IHK-Beitragsrückständen durch ein zu beauftragendes Inkasso-Unternehmen datenschutzrechtlich zu beurteilen ist.

Zunächst war darauf hinzuweisen, dass sich die Verarbeitung personenbezogener Daten im Auftrag nach § 4 LDSG richtet. Die auftraggebende Stelle (IHK) bleibt demnach für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Die näheren Bedingungen der Auftragsdatenverarbeitung sind vertraglich mit dem Auftragnehmer festzulegen. Der Auftragnehmer ist diesbezüglich weisungsabhängig gegenüber dem Auftraggeber, der Herr der Daten bleibt.

Bislang erfolgt die Beitreibung von IHK-Beitragsrückständen durch die Gemeinden nach den für Gemeindeabgaben geltenden Bestimmungen. In diesem Zusammenhang ergibt sich aus § 3 Abs. 8 IHK-Gesetz, dass die landesrechtlichen Vorschriften entsprechend anzuwenden sind. Nach § 108 Abs. 1 GemO ist es grundsätzlich auch möglich, Kassengeschäfte ganz oder zum Teil von einer Stelle außerhalb der Gemeindeverwaltung besorgen zu lassen. Bei den gemeindlichen Kassengeschäften werden häufig auch sensible personenbezogene Daten (z. B. aus Bußgeldverfahren, aus Abgabenbescheiden oder aus Vollstreckungsaufträgen) verarbeitet. Daher wäre wohl die IHK grundsätzlich befugt, zwecks Beitreibung von Beitragsrückständen eine andere Stelle – hier ein Inkasso-Unternehmen – zu beauftragen mit der Maßgabe, dass die vertragliche Gestaltung der Auftragsdatenverarbeitung den datenschutzrechtlichen Bestimmungen Rechnung trägt.

Nach Kenntnis der konkreten Rahmenbedingungen musste die Einziehung von Außenständen säumiger IHK-Mitglieder auch weiterhin durch die Gemeinden erfolgen.

14.5 Arbeitszeit in Krankenhäusern

Die rheinland-pfälzische Gewerbeaufsicht plante, im Herbst 2002 eine Überprüfung der Arbeitszeiten der Beschäftigten in den Krankenhäusern durchzuführen. Dabei sollten die Arbeitszeitnachweise der betroffenen Mitarbeiterinnen und Mitarbeiter stichprobenhaft kontrolliert werden. Der LfD wurde vor Beginn der Schwerpunktaktion „Arbeitszeit in Krankenhäusern“ von einem Verein, der die Interessen der Krankenhäuser vertritt, gebeten zu prüfen, ob hinsichtlich der Übersendung der angeforderten Listen der Beschäftigten datenschutzrechtliche Bedenken bestehen.

Hier war zunächst darauf hinzuweisen, dass nach allgemeiner Auffassung Name, Dienstbezeichnung und Funktionsbeschreibung der Bediensteten Informationen sind, die grundsätzlich nicht dem informationellen Selbstbestimmungsrecht unterliegen. Diese Angaben gehören nämlich nicht primär zur Individualsphäre der Bediensteten, sondern haben einen engen Bezug zur beruflichen Tätigkeit. Um in diesem Bereich die Abgrenzung zu verdeutlichen: Soweit die Information auch die Veröffentlichung eines Bildes beträfe, wenn das Geburtsdatum, die Privatadresse oder das Privattelefon in Rede stünden, würden diese Daten sicherlich dem informationellen Selbstbestimmungsrecht der Bediensteten unterliegen, da sie in deren persönlicher Sphäre angesiedelt sind. Vorliegend kommt hinzu, dass die von der Aufsichtsbehörde angeforderten „Grunddaten“ der Mitarbeiter (Name, Tätigkeitsbereich) in aller Regel frei zugänglich sind. Als Beispiel sei das Internetangebot der Universitätsklinik Mainz genannt. Dort sind nicht nur die Namen der Mitarbeiter und deren Tätigkeitsbereiche angeführt, sondern darüber hinaus auch Informationen zur Erreichbarkeit wie Telefondurchwahl, Gebäudebezeichnung bis hin zur Zimmernummer.

Dies vorausgeschickt, hat der LfD die Anfrage wie folgt beantwortet:

Das Auskunftsbegehren der Gewerbeaufsicht stützt sich auf die entsprechenden Regelungen des Arbeitszeitgesetzes. Zweck des Gesetzes ist es, die Sicherheit und den Gesundheitsschutz der Arbeitnehmer bei der Arbeitszeitgestaltung zu gewährleisten sowie Tage der Arbeitsruhe der Arbeitnehmer zu schützen (vgl. § 1 ArbZG). Nach § 17 Abs. 4 ArbZG kann die Aufsichtsbehörde vom Arbeitgeber die für die Durchführung des Gesetzes erforderlichen Auskünfte verlangen und ihm aufgeben, die Arbeitszeitnachweise vorzulegen oder zur Einsicht einzusenden. Die Vorschrift soll insbesondere der Bekämpfung von Arbeitszeitverstößen dienen. Eines Anlasses für die Kontrolle bedarf es nicht. Auf dieser gesetzlichen Grundlage könnte sich die Aufsichtsbehörde sämtliche Arbeitszeitnachweise vorlegen oder zuschicken lassen. Diese Nachweise enthalten u. a. den Namen und den Tätigkeitsbereich der Betroffenen. Es bestünde hier also die Möglichkeit, lückenlos nachzuforschen und auszuwerten.

Im vorliegenden Fall hatte die Aufsichtsbehörde indessen einen wesentlich geringeren Eingriff geplant, nämlich lediglich eine Stichprobe, zu deren Vorbereitung die angeforderten Listen der Beschäftigten – beschränkt auf Namen und Tätigkeitsbereich – dienten. Zur Erforderlichkeit führte das Ministerium für Arbeit, Soziales, Familie und Gesundheit ergänzend aus, dass „durch die schriftliche Anforderung der Auskünfte ein zusätzlicher Aufwand für alle Beteiligten vermieden werden soll. Andernfalls müsste in jedem der betroffenen Krankenhäuser ein zusätzlicher Besprechungstermin zwischen Gewerbeaufsicht und der betroffenen Krankenhausleitung vereinbart werden, bei dem eine Auswahl der betreffenden Mitarbeiterinnen und Mitarbeiter, deren Arbeitszeiten stichprobenhaft kontrolliert werden, bestimmt wird.“ Damit war die Erforderlichkeit hinreichend konkret dargelegt. Unter mehreren geeigneten Möglichkeiten zur Erreichung ihres Ziels (Kontrolle der Arbeitszeit mittels Stichprobe) kann die Aufsichtsbehörde

– wie hier geschehen – grundsätzlich nach ihrem Ermessen wählen. In diesem Zusammenhang hat das Ministerium versichert, dass die erbetenen Listen nur zu vorgenanntem Zweck benötigt und nach Abschluss der Aktion nicht weiter verwendet werden. Es sind also flankierend verfahrensmäßige Vorkehrungen getroffen worden, die eine weiter gehende Nutzung verhindern.

Nach allem hatte die Datenanforderung durch die Aufsichtsbehörde unter keinem Gesichtspunkt zu einer unzulässigen Offenbarung personenbezogener Daten geführt.

14.6 Änderungen der Fahrerlaubnis-Verordnung

Schon bald nach In-Kraft-Treten der Fahrerlaubnis-Verordnung am 1. Januar 1999 ergab sich bei der praktischen Anwendung die Notwendigkeit verschiedener Änderungen und Ergänzungen, die zur Vorbereitung einer – am 1. September 2002 in Kraft getretenen – Änderungsverordnung durch das Bundesministerium für Verkehr, Bau und Wohnungswesen führte. Datenschutzrechtlich bedeutsam ist im Bereich „Kraftfahreignung“ die ergänzte Vorschrift des § 11 Abs. 6 Satz 2 FeV über die Darlegungspflicht der Fahrerlaubnisbehörde gegenüber den Betroffenen. Neu aufgenommen wurde die Pflicht, dem Betroffenen ausdrücklich mitzuteilen, dass er die an die untersuchende Stelle zu übersendenden Unterlagen einsehen kann. Damit soll der Tatsache Rechnung getragen werden, dass der Betroffene als Auftraggeber des Gutachtens die Möglichkeit haben muss, sich über den Inhalt der Unterlagen zu informieren. Zugleich soll die ergänzende Regelung – wie es in der Begründung zur FeV-ÄnderungsVO (vgl. Bundesratsdrucksache 497/02, S. 63) zum Ausdruck kommt – der Transparenz des Verwaltungshandelns dienen.

14.7 Feststellung der Kraftfahreignung durch die Fahrerlaubnisbehörde

Die anzuwendenden Regelungen über die Eignung zum Führen von Kraftfahrzeugen und das Vorgehen der Fahrerlaubnisbehörde bei der zu prüfenden Eignung sind immer wieder Gegenstand von Eingaben und Anfragen. Aufgrund oftmals herrschender Unklarheiten (sowohl auf Seiten der Petenten als auch bei den Behörden) werden im Folgenden jene zentralen Vorschriften und Leitlinien dieses Komplexes dargestellt, die häufig zu Anwendungsproblemen geführt haben.

– Gemäß § 2 Abs. 4 Satz 1 StVG ist geeignet zum Führen von Kraftfahrzeugen, wer die notwendigen körperlichen und geistigen Anforderungen erfüllt und nicht erheblich oder nicht wiederholt gegen verkehrsrechtliche Vorschriften oder gegen Strafgesetze verstoßen hat. Die körperliche und geistige Eignung ist damit nur unvollkommen beschrieben. Denn es bleibt nach wie vor unbestimmt, welche Anforderungen „notwendig“ sind.

– Die Fahrerlaubnisverordnung enthält auf der Grundlage der in § 6 Abs. 1 Nr. 1 c StVG erteilten Ermächtigung nähere Konkretisierungen des Begriffs der Kraftfahreignung. Was die körperliche und geistige Eignung anbelangt, bestimmt § 11 Abs. 1 Satz 2 FeV, dass die Anforderungen insbesondere dann nicht erfüllt sind, wenn eine Erkrankung oder ein Mangel nach Anlage 4 vorliegt, wodurch die Eignung zum Führen von Kraftfahrzeugen ausgeschlossen wird. Diese Anlage trifft keine abschließende Regelung, weder hinsichtlich der Aufzählung der Krankheiten und Mängel noch inhaltlich in Bezug auf die Bewertung der Eignung bzw. Nichteignung. In den Vorbemerkungen zu Anlage 4 wird vielmehr darauf hingewiesen, dass sie nur häufiger vorkommende Erkrankungen und Mängel enthält, die die Eignung zum Führen von Kraftfahrzeugen längere Zeit beeinträchtigen oder aufheben können.

– Wesentliche Anhaltspunkte für die Präzisierung des Begriffs der Kraftfahreignung enthalten die Begutachtungsleitlinien zur Kraftfahreignung des Gemeinsamen Beirats für Verkehrsmedizin beim Bundesministerium für Verkehr, Bau- und Wohnungswesen und beim Bundesministerium für Gesundheit (Berichte der Bundesanstalt für Straßenwesen, Mensch und Sicherheit, Heft M 115, Bergisch-Gladbach, Februar 2000). Diese Leitlinien bieten eine Zusammenstellung eignungsausschließender und eignungseinschränkender körperlich-geistiger (psychischer) und charakterlicher Mängel beim Fahrerlaubnisbewerber und Fahrerlaubnisinhaber aufgrund ärztlicher und verkehrspsychologischer Erkenntnisse und Erfahrungen. Alle aufgeführten Beurteilungsleitsätze und -begründungen beruhen auf eingehenden Beratungen unter Einbeziehung aktueller Stellungnahmen aller relevanten medizinischen und psychologischen Fachgesellschaften sowie gutachterlichen Erfahrungen.

– Teilweise unterscheiden sich die Aussagen der Begutachtungsleitlinien zur Kraftfahreignung von den Aussagen in der oben erwähnten Anlage 4 der Fahrerlaubnisverordnung. Maßgebend sind allerdings die Begutachtungsleitlinien zur Kraftfahreignung. Die darin zusammengefassten Erkenntnisse sind nach Auffassung des OVG Rheinland-Pfalz (VRS 99, S. 238) in die Fahrerlaubnisverordnung integriert und damit normativ als für den Regelfall zutreffend gekennzeichnet.

– Mitunter sind hinsichtlich der Eignungsprüfung behördliche Ermittlungen notwendig. Liegen nämlich Eintragungen im Verkehrszentralregister bzw. im Bundeszentralregister vor, werden die Akten, die Auskunft über die Vorgänge geben, eingesehen und daraufhin analysiert, ob sie Hinweise auf Einbußen der Fahreignung enthalten.

– Häufig weist der LfD im Rahmen von Eingaben darauf hin, dass die Polizei Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden nach § 2 Abs. 12 Satz 1 StVG zu übermitteln hat, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist. Diese Vorschrift ist in

das StVG aufgenommen worden, weil die Zulässigkeit solcher Datenübermittlungen nach den Polizeigesetzen der Länder unterschiedlich beurteilt wird, die Datenübermittlung jedoch nach Auffassung der Bundesregierung (Bundesratsdrucksache 821/96, S. 51) aus Gründen der Verkehrssicherheit unerlässlich ist.

– Problematisch sind oft Sachverhalte, bei denen es um Mitteilungen von Ärzten geht. Der Arzt ist durch die Schweigepflicht, deren Verletzung durch § 203 StGB mit Strafe bedroht ist, gehindert, die Fahrerlaubnisbehörde ohne Einwilligung des Patienten über von ihm beobachtete Eignungsmängel in Kenntnis zu setzen. Vom Bewerber um eine Fahrerlaubnis oder vom Inhaber einer Fahrerlaubnis kann die Entbindung des Arztes von seiner Schweigepflicht seitens der Fahrerlaubnisbehörde nicht gefordert werden. Ein Arzt kann aber trotz seiner grundsätzlichen Schweigepflicht nach den Grundsätzen über die Abwägung widerstreitender Pflichten oder Interessen berechtigt sein, die Fahrerlaubnisbehörde zu benachrichtigen, wenn sein Patient mit einem Kfz am Straßenverkehr teilnimmt, obwohl er wegen seiner Erkrankung nicht mehr fähig ist, ein Kraftfahrzeug zu führen, ohne sich und den öffentlichen Verkehr zu gefährden. Voraussetzung dafür ist jedoch, dass der Arzt zunächst den Patienten auf seinen Zustand und auf die Gefahren aufmerksam macht, die sich beim Führen eines Kfz ergeben. Werden einem Amtsarzt bei seiner Amtstätigkeit Informationen über das Vorliegen von eignungsausschließenden oder die Fahreignung erheblich einschränkenden Mängeln bei Personen, die eine Fahrerlaubnis besitzen, bekannt, wird er sie in der Regel an die Fahrerlaubnisbehörde weitergeben. Dabei wird der Schutz von Leib und Leben der Verkehrsteilnehmer als höheres Rechtsgut gegenüber dem Schutz personenbezogener Daten angesehen. In diesem Zusammenhang wird allgemein das Spannungsverhältnis zwischen präventiver Gefahrenabwehr und allgemeinem Persönlichkeitsrecht (Art. 2 Abs. 1 GG) deutlich.

– Das Fahrerlaubnisrecht unter dem Aspekt der verkehrsbezogenen Gefahrenabwehr enthält Grundlagen für die vorbeugende Abwehr von Verkehrsgefahren durch Kraftfahrer. Aufgrund der Schutzpflicht (Art. 2 Abs. 2 GG) für bedeutende Rechtsgüter wie Gesundheit und Leben von Verkehrsteilnehmern ist der Staat verpflichtet, rechtzeitig Maßnahmen zu ergreifen, wenn Tatsachen bekannt werden, die Bedenken gegen die Eignung des Fahrerlaubnisbewerbers oder -inhabers begründen (§ 2 Abs. 8 StVG). Mit Rücksicht auf diesen Auftrag sind die zuständigen Straßenverkehrsbehörden nach Kenntnisnahme von verkehrsrelevanten Tatsachen zu entsprechenden Maßnahmen verpflichtet.

– Die Fahrerlaubnisbehörde legt unter Berücksichtigung der Besonderheiten des Einzelfalls gem. § 11 Abs. 6 Satz 1 FeV fest, welche Fragen im Hinblick auf die Eignung des Betroffenen zum Führen von Kraftfahrzeugen zu klären sind. Diese Vorschrift zwingt die Fahrerlaubnisbehörde zu exakter Formulierung der Fragen, die der Aufklärung bedürfen. Die Fragestellung der Behörde charakterisiert den Untersuchungsanlass und bestimmt damit Ausmaß und Umfang der Untersuchung.

14.8 Sonstiges aus dem Bereich Kraftfahrzeug und Straßenverkehr

Erwähnenswertes aus dem Berichtszeitraum ist im Folgenden dargestellt:

14.8.1 Datenübermittlung der Kraftfahrzeug-Zulassungsstelle an Privatpersonen

In Eingaben wird oft bemängelt, dass Privatpersonen Halterauskünfte bekommen. Meistens ist nach dem jeweils vorgetragenen Sachverhalt die Datenübermittlung zulässig.

So dürfen nach der Regelung in § 39 StVG Auskünfte aus dem Halterregister der Kfz-Zulassungsstelle auch an Private erteilt werden, wenn der Anfragende einen Rechtsanspruch geltend macht, der im Zusammenhang mit der Teilnahme am Straßenverkehr steht. Ob der Anspruch letztlich durchsetzbar sein wird, ist für die Auskunftserteilung unerheblich.

In den Erläuterungen zu § 39 StVG ist im Verkehrsblatt 1993, S. 525 (amtlicher Teil) zu dem Erfordernis der Darlegung, warum Auskunft erteilt werden soll, Folgendes ausgeführt:

„Darlegung bedeutet plausible Behauptung, annehmbare Erläuterung, schlüssiger, widerspruchsfreier Vortrag eines Sachverhalts, aus dem sich ein Anspruch ergeben kann. Es genügt, wenn der Antragsteller erklärt, dass er ‚… durch ein bestimmtes Ereignis im Straßenverkehr …' geschädigt ist und zur Geltendmachung von Schadensersatzansprüchen die Daten benötigt. Anzugeben sind dazu Zeitpunkt und möglichst Ort des Schadensereignisses."

Diese Voraussetzungen werden seitens der Auskunftsbegehrenden gegenüber der Zulassungsstelle in aller Regel erfüllt.

14.8.2 Kfz-Halter-Daten für das Sozialamt

Zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe ermächtigt § 117 Abs. 3 BSHG die Träger der Sozialhilfe, Daten u. a. zur „Eigenschaft als Kraftfahrzeughalter" zu erheben (vgl. dazu im Einzelnen 17. Tb., Tz. 11.2.6.2). In diesem Zusammenhang war bislang problematisch, auf welcher Grundlage die Straßenverkehrsbehörden Antworten übermitteln durften. Seit dem 1. Januar 2003 findet sich die normenklare Rechtsgrundlage für solche Übermittlungen nunmehr in § 35 Abs. 5 Nr. 6 StVG i. V. m. § 9 a Fahrzeugregisterverordnung.

14.8.3 Datenspeicherung bei gezahltem Verwarnungsgeld?

Ein Petent rügte einen datenschutzrechtlichen Verstoß anlässlich eines Verwarnungsgeldverfahrens. Das Verwarnungsgeld sei von ihm fristgerecht gezahlt worden. Aufgrund seiner entsprechenden Anfrage beim Ordnungsamt habe er die Mitteilung erhalten, dass die in jenen Verfahren erhobenen personenbezogenen Daten üblicherweise drei Jahre lang gespeichert würden. Diese Verfahrensweise sei seines Erachtens jedoch nicht erforderlich.

Hier wies der LfD das (einsichtige) Ordnungsamt darauf hin, dass es im Straßenverkehrsgesetz keine Rechtsgrundlage gibt, die es den örtlichen Behörden erlaubt, erteilte Verwarnungen wegen Zuwiderhandlungen im ruhenden Verkehr zu speichern. Eine solche Regelung wäre auch bedenklich; denn bei der Erteilung einer Verwarnung wird dem Betroffenen das Fehlverhalten nur vorgehalten, ohne darüber zu entscheiden. Das Verwarnungsgeld wird mit seinem Einverständnis erteilt, ohne dass seine Täterschaft oder das Vorliegen der Ordnungswidrigkeit formell festgestellt werden. Mit dieser Konzeption des Verwarnungsgeldverfahrens ist die Zulassung einer örtlichen Speicherung nicht vereinbar.

14.8.4 Verjährung bei Verkehrsordnungswidrigkeitenverfahren

Ein Petent trug vor, dass ihm eine Verkehrsordnungswidrigkeit zur Last gelegt werde. Obwohl die Tat bereits mehr als drei Monate zurückliegen würde, werde gegen seine Person ermittelt.

Hier wäre – so teilte der LfD dem Petenten mit – die Erforderlichkeit von Datenerhebungen zur Feststellung des verantwortlichen Fahrers dann nicht gegeben, wenn eine Verfolgungsverjährung eingetreten ist. Die Verjährungsfrist beträgt nach § 26 Abs. 3 StVG drei Monate, solange weder ein Bußgeldbescheid ergangen noch öffentliche Klage erhoben worden ist. Nach § 33 Abs. 1 Nr. 1 OWiG tritt allerdings eine Verjährungsunterbrechung ein, wenn dem Betroffenen bekannt gegeben worden ist, dass gegen ihn ein Ermittlungsverfahren geführt wird. Eine solche Bekanntgabe liegt vor, wenn dem Betroffenen ein Anhörungsbogen mit konkreten Angaben zur Person und zum Tatvorwurf – wie im geschilderten Fall geschehen – übersandt wird. Eine Verfolgungsverjährung war nicht eingetreten.

15. Landwirtschaft, Weinbau und Forsten

15.1 Anzeigepflicht nach dem Futtermittelgesetz

Das LUFA in Speyer untersucht im Auftrag Futtermittelproben auf die Einhaltung der zulässigen Grenzwerte. Es fragte an, inwieweit eine Anzeigepflicht bestehe, wenn Überschreitungen der Grenzwerte festgestellt würden, und gab dabei zu bedenken, dass den Auftraggebern vertraglich ein vertraulicher Umgang mit den Daten zugesichert worden sei.

Das Futtermittelgesetz sieht eine unverzügliche Informationspflicht durch diejenigen vor, die beruflich oder gewerbsmäßig mit Futtermitteln umgehen, wenn die Belastung mit unerwünschten Stoffen bei Verfütterung eine schwerwiegende Gefahr für Menschen oder Tiere darstellen würde. Zweck des Gesetzes ist es, Menschen und Tiere vor gesundheitlichen Beeinträchtigungen zu schützen, die durch Verwendung von fehlerbehafteten Futtermitteln auftreten können. Daher sind alle diejenigen zur Weitergabe von Informationen verpflichtet, die aufgrund ihres Umgangs mit Futtermitteln beurteilen können, ob zulässige Grenzwerte bei den Inhaltsstoffen überschritten werden. Damit sind nicht nur z. B. die Futtermittelhersteller oder -vertreiber aufgefordert, sondern auch Institutionen, die Futtermittelüberprüfungen vornehmen, da auch diese beruflich mit Futtermitteln umgehen. Folglich bestand auch für das LUFA eine unverzügliche Informationspflicht nach dem Futtermittelgesetz. Wer eine rechtzeitige Unterrichtung unterlässt, handelt ordnungswidrig. Dabei war es unerheblich, dass vertraglich ein vertraulicher Umgang mit den Daten zugesichert wurde. Denn eine gesetzliche Informationspflicht kann durch einen privatrechtlichen Vertrag nicht ausgeschlossen werden.

15.2 Nutzung der Weinbaukartei

Der Bürgermeister einer Verbandsgemeinde beabsichtigte, zur Vorbereitung einer Broschüre die Weinbaubetriebe eines bestimmten Bereichs anzuschreiben. Hierzu benötigte er die Anschriften aus der Weinbaukartei.

Die Weinbaukartei findet ihre Grundlage in der Verordnung (EWG) Nr. 2392/86 des Rates vom 24. Juli 1986, wonach die Mitgliedstaaten dafür Sorge zu tragen haben, dass die Weinbaukartei ausschließlich zur Durchführung der weinrechtlichen Vorschriften oder für statistische Zwecke oder strukturelle Maßnahmen verwendet wird. Nur wenn es ihre innerstaatlichen Rechtsvorschriften zulassen, können die Mitgliedstaaten vorsehen, dass die Kartei auch zu anderen Zwecken verwendet werden kann, insbesondere zu strafrechtlichen oder steuerlichen Zwecken. Eine Datenübermittlung an den Bürgermeister durch die Landwirtschaftskammer aus der Kartei war daher nicht zulässig, da sie weder der Durchführung weinrechtlicher Vorschriften noch statistischen Zwecken oder strukturellen Maßnahmen diente. Es bestehen auch keine innerstaatlichen Rechtsvorschriften, die hier eine Ausnahme zugelassen hätten. Um dennoch die Winzer erreichen zu können, wurde dem Bürgermeister eine sog. Datenmittlung vorgeschlagen. Dies bedeutet, dass die Landwirtschaftskammer für ihn ein Anschreiben an die Winzer versendet und diese sich sodann, sofern sie es möchten, mit dem Bürgermeister in Verbindung setzen können.

16. Statistik

16.1 Der jährliche Mikrozensus

Der Mikrozensus ist eine seitens des Statistischen Landesamtes durchgeführte amtliche Haushaltsbefragung, mit der insbesondere wichtige Ergebnisse über die wirtschaftliche und soziale Lage der Bevölkerung ermittelt werden. Diesbezüglich werden die Angaben von Bürgerinnen und Bürgern, die in repräsentativ ausgewählten Befragungsbezirken wohnen, benötigt. Regelmäßig erreichen den LfD in diesem Zusammenhang zahlreiche Anfragen aus der Bevölkerung.

Die amtliche Statistik führt statistische Erhebungen nur dann durch, wenn sie durch Gesetz oder andere Rechtsvorschriften angeordnet sind. Die Rechtsgrundlage für den Mikrozensus ist das Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz). Nach einer objektiven, mathematisch-statistischen Zufallsauswahl wurden aus den etwa 37 Millionen Haushalten in Deutschland 370 000 Haushalte ausgewählt. Ausgehend von den Ergebnissen der Volkszählung 1987 wird das Bundesgebiet in Flächen mit etwa gleich vielen Wohnungen eingeteilt. Von diesen Flächen – den so genannten Auswahleinheiten – wird dann ein Prozent mit Hilfe von Zufallszahlen in einem voll automatischen Verfahren ermittelt. Dies sind die so genannten Auswahlbezirke. Jede Fläche hat dabei die gleiche Chance (Wahrscheinlichkeit), ausgewählt zu werden. Alle in den ausgewählten Flächen wohnenden Haushalte werden in die Erhebung einbezogen. Der Mikrozensus umfasst einerseits Merkmale, die der Auskunftspflicht unterliegen, andererseits aber auch Fragen, deren Beantwortung freiwillig ist. Für Haushaltsmitglieder, die wegen ihrer Behinderung selbst nicht Auskunft geben können, ist jedes andere auskunftspflichtige Haushaltsmitglied zur Auskunft verpflichtet. Widerspruch und Anfechtungsklage gegen die Aufforderung zur Auskunftserteilung haben gem. § 15 Abs. 6 BStatG keine aufschiebende Wirkung. Um den Betroffenen das Ausfüllen der Erhebungsvordrucke zu erleichtern, werden Interviewer und Interviewerinnen eingesetzt. Sie sind Erhebungsbeauftragte des Statistischen Landesamtes, müssen sich durch einen Interviewerausweis in Verbindung mit dem Personalausweis ausweisen und dürfen die Wohnung nur mit Zustimmung eines Verfügungsberechtigten betreten. Ebenso wie alle im Statistischen Landesamt mit dem Mikrozensus beschäftigten Mitarbeiterinnen und Mitarbeiter sind auch die Interviewer nach § 16 Abs. 1 BStatG zur absoluten Verschwiegenheit verpflichtet. Das Statistische Landesamt ist nach den Feststellungen des LfD sehr darauf bedacht, keine Interviewer einzusetzen, bei denen ein Interessenkonflikt aufgrund ihrer beruflichen oder dienstlichen Tätigkeit denkbar wäre. Auch wird darauf geachtet, keine Interviewer einzusetzen, die in unmittelbarer Nachbarschaft des betroffenen Wohngebietes wohnen. Die interviewenden Personen dürfen aus der Interviewertätigkeit im Rahmen der Mikrozensuserhebung gewonnene Erkenntnisse nicht in anderen Verfahren oder für andere Zwecke verwenden. Sollten die Betroffenen dennoch Bedenken haben, die erforderlichen Angaben dem Interviewer gegenüber direkt zu machen, so können sie gem. § 8 Mikrozensusgesetz den Fragebogen auch selbst ausfüllen und ihre Angaben in einem verschlossenen Umschlag an das Statistische Landesamt übersenden.

16.2 Erste Ergebnisse des Zensustests

Wie bereits im 18. Tb. dargestellt, wird gegenwärtig auf der Grundlage des Gesetzes zur Vorbereitung eines registergestützten Zensus vom 27. Juli 2001 (BGBl. I S. 1882) getestet, ob die Dateien der Verwaltung geeignet sind, bei künftigen Volkszählungen die Befragungen der Bürger zu ersetzen. Die von den Datenschutzbeauftragten des Bundes und der Länder diesbezüglich eingebrachten datenschutzrechtlichen Erfordernisse wurden berücksichtigt (vgl. im Einzelnen 18. Tb., Tz. 16.1).

Der am 5. Dezember 2001 durchgeführte Zensustest sollte Auskunft geben über die Möglichkeiten, bisherige Totalerhebungen in Form von Gebäude- und Wohnungszählungen sowie Volks- und Berufszählungen durch registergestützte Erhebungsformen zu ersetzen. Dazu wurden Daten aus Melderegistern und Dateien der Bundesanstalt für Arbeit herangezogen und mit originär erhobenen Daten zusammengeführt und verglichen. Eine bedeutende Aufgabe des registergestützten Zensus ist die Feststellung der amtlichen Einwohnerzahl. Deshalb war es notwendig, die Tauglichkeit der Melderegister für ein solches Vorhaben zu überprüfen. In einem Test wurde festgestellt, in welchem Umfang in den Melderegistern „Karteileichen“ (Personen, die im Melderegister geführt, gemäß Haushaltebefragung aber nicht wohnhaft sind) enthalten sind. Im Rahmen des Registertests wurden von den Stichprobengemeinden zwei im Abstand von vier Monaten erstellte Melderegisterauszüge (erste und zweite Datenlieferung) ausgewählter Gebäude bereitgestellt, zusammengeführt und mit den Ergebnissen der Haushaltebefragung (vgl. dazu Tz. 3.1) in den ausgewählten Gebäuden abgeglichen. Die auf dieser Grundlage seitens des Statistischen Landesamtes ermittelte „Karteileichenrate“ lag bei 1,6 Prozent.

Als Zwischenergebnis konnte festgestellt werden, dass sich die Anordnung von zwei Datenlieferungen bewährt hat und auch bei einem künftigen registergestützten Zensus erfolgen sollte. Mit Hilfe von zwei Datenlieferungen, die mehrere Monate auseinander liegen, können falsche Zuordnungen des Wohnsitzes vermieden werden. Ein abschließender Bericht mit entsprechenden Empfehlungen zur weiteren Vorgehensweise ist zum Jahresende 2003 angekündigt.

17. Personaldatenschutz, Vorbemerkung

Datenschutzfragen tauchen nicht nur im Verhältnis Staat/Bürger auf, auch und gerade im Dienst- und Arbeitsverhältnis ist häufig zu spezifischen Fragen des Arbeitnehmerdatenschutzes Stellung zu nehmen. Es geht dabei meistens darum zu klären, wo die Grenze zwischen den legitimen Kontrollrechten des Arbeitgebers und dem informationellen Selbstbestimmungsrecht der Beschäftigten zu ziehen ist.

Auf Bundesebene fordern Datenschutzbeauftragte und Gewerkschaften seit langem, die aktuellen datenschutzrelevanten Fragen im Bereich des Arbeitslebens gesetzlich zu regeln. Zum Erlass eines eigenständigen Arbeitnehmerdatenschutzgesetzes ist es jedoch trotz zahlreicher Ankündigungen der Bundesregierung – letztmals im Koalitionsvertrag zwischen SPD und BÜNDNIS 90/DIE GRÜNEN vom 16. Oktober 2002 – bislang nicht gekommen.

Die Zulässigkeit der Verarbeitung von Telefon- bzw. Internetverbindungsdaten bildet dabei nicht selten einen Streitpunkt zwischen Dienststelle und Beschäftigten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zur datenschutzgerechten Nutzung von E-Mail- und anderen Internet-Diensten am Arbeitsplatz eine Entschließung gefasst (vgl. Anlage 9 und ergänzend Anlage 31), welche sich ausführlich mit der Thematik befasst.

17.1 Beihilfe-Outsourcing; Urteil des OVG Rheinland-Pfalz

Nicht nur in Rheinland-Pfalz, sondern auch in anderen Ländern besteht seit Jahren die Praxis, die Berechnung und Zahlbarmachung der Beihilfe auf externe Dienstleister zu übertragen. Der LfD hatte seine Vorbehalte gegen die Beauftragung privater Dienstleister dabei stets deutlich zum Ausdruck gebracht (vgl. 18. Tb. Tz. 17.2). Auch das OVG Münster hatte in seinem Beschluss vom 28. August 1997 (vgl. RDV 1998, S. 71) die Beauftragung Privater als unzulässig bewertet. Gleichwohl sah man im Hinblick auf die unterschiedlichen landesrechtlichen Bestimmungen und den vorläufigen Charakter des Beschlusses im Land keinen Änderungsbedarf. Dieser ergab sich jedoch mit dem Urteil des OVG Rheinland-Pfalz vom 19. April 2002 (vgl. ZBR 2002 S. 368), in welchem das Gericht Inhalt und Grenzen bei der Beauftragung privater Unternehmen deutlich aufzeigte.

Im konkreten Fall hatte sich ein Pensionär dagegen gewandt, dass eine Verbandsgemeinde das Beihilfeberechnungszentrum GmbH (bbz) mit der Berechnung und Zahlbarmachung der Beihilfe beauftragt hatte. Das OVG ging in seinem Urteil allerdings davon aus, dass es sich bei dem bbz um eine private Stelle handelt. Da sich das bbz jedoch zu 100 % in der Trägerschaft der evangelischen Kirche befindet, handelt es sich datenschutzrechtlich um eine öffentliche Stelle, welche als Auftragnehmer gegenüber privaten Dienstleistern grundsätzlich privilegiert ist. In dem Urteil führt das Gericht aus, dass von bloßen Verwaltungshilfstätigkeiten keine Rede sein könne, es aber andererseits für die erfolgte Zuständigkeitsverlagerung an einer gesetzlichen Grundlage fehle. Die Vorschriften zum Personalaktenrecht seien als abschließende Sonderregelung zu begreifen, die schon wegen des Abschottungsgebotes eine Sperrwirkung im Bezug auf eine Auslagerung entfalteten.

Der LfD sieht sich durch dieses Urteil in seinen Vorbehalten gegen die Beauftragung privater Unternehmen und in seiner Forderung nach einer normenklaren Rechtsgrundlage für das Beihilfe-Outsourcing nachdrücklich bestätigt (vgl. 18. Tb., Tz 17.2).

Mehr als 80 % der Kommunen in Rheinland-Pfalz haben die Berechnung und Zahlbarmachung der Beihilfe ausgelagert. Häufig ist dies mit dem Abschluss einer Beihilfeversicherung verbunden, um den Gemeindehaushalt vor unvorhersehbaren hohen Beihilfekosten zu schützen. Beauftragen die Kommunen dabei kommunale Versorgungskassen, weil sie die Beihilfebearbeitung insgesamt auslagern wollen und wegen der geringen Zahl von Beamten an dem Abschluss einer Rückversicherung kein Interesse haben, findet sich in § 63 der Gemeindeordnung bereits die entsprechende Rechtsgrundlage.

Um den Vorgaben des OVG gerecht zu werden, ist in den anderen Fällen durch eine Änderung des Landesbeamtengesetzes die Rechtsgrundlage für die Beauftragung externer Dienstleister noch zu schaffen. Ursprünglich war vorgesehen, die Beauftragung privater Versicherungen im Wege der Beleihung zu ermöglichen, wobei der Abschluss der Versicherung an die Beihilfebearbeitung gekoppelt werden sollte. Datenschutzrechtlich hatte dies den Vorteil, dass die Einschaltung von Subunternehmen ausgeschlossen und der Kreis der zugriffsberechtigten Personen möglichst klein gehalten wurde. Im Laufe des Gesetzgebungsverfahrens wurde jedoch von verschiedenen Seiten die vollständige Öffnung für den privaten Bereich aus Gründen des freien Wettbewerbs gefordert. Derzeit ist beabsichtigt, die Beleihung privater Unternehmen zu gestatten, welche eine Versicherung zwar nicht selbst anbieten, aber vermitteln. Aus datenschutzrechtlicher Sicht ist dabei zu fordern, dass die Weitergabe von Beihilfedaten an den Versicherer auf anonymisierte Daten beschränkt bleibt. Der LfD hat sich in diesem Sinne in das Gesetzgebungsverfahren eingebracht und wird die weitere Entwicklung kritisch begleiten.

17.2 Datenschutz im Bewerbungsverfahren

Im Berichtszeitraum rückte der Datenschutz im Bewerbungsverfahren wiederholt in den Mittelpunkt der Betrachtung. Es ging z. B. darum, welche Informationen ein künftiger Arbeitgeber von dem Bewerber erfragen, mithin erheben darf, sowie um den Informationsaustausch zwischen ehemaligem und künftigem Arbeitgeber.

17.2.1 Die Frage nach den Schulden des Bewerbers

In einem von der ADD eingesetzten Formular sollte der Bewerber zusätzlich zur Bestätigung, dass er „mit seiner Familie in geordneten Verhältnissen lebe“, Art und Höhe seiner Schulden beziffern.

In der Verwaltungsvorschrift über die Vorlage von Führungszeugnissen und Einholung von unbeschränkten Auskünften aus dem Zentralregister bei der Einstellung in den Landesdienst vom 18. Dezember 1991 (MinBl. S. 32) ist die Frage nach den wirtschaftlichen Verhältnissen bzw. nach konkreten Schulden zwar ausdrücklich vorgesehen. Der LfD vertritt in Übereinstimmung mit dem Ministerium des Innern und für Sport jedoch die Auffassung, dass es im Regelfall ausreicht, lediglich eine Erklärung zu verlangen, dass der Bewerber in geordneten wirtschaftlichen Verhältnissen lebt und Zwangsvollstreckungsmaßnahmen gegen ihn nicht betrieben werden. Konkrete Angaben zur Art und Höhe von bestehenden Verbindlichkeiten sind allenfalls dann erforderlich, wenn die Einstellung in Tätigkeitsbereichen erfolgen soll, die eine besondere Vertrauensstellung voraussetzen. Dies ist z. B. der Fall bei Tätigkeiten in sicherheitsempfindlichen Bereichen (Polizei, Verfassungsschutz), in korruptionsanfälligen Bereichen (Beschaffungswesen) oder auch in solchen Bereichen, in denen öffentliche Gelder verwaltet werden (z. B. Kassenwesen, Buchhaltung). Das Ministerium des Innern und für Sport unterrichtete den nachgeordneten Bereich über seine Rechtsauffassung und kündigte an, eine entsprechende Klarstellung der o. g. Verwaltungsvorschrift bei der im Jahr 2004 anstehenden Überarbeitung vorzunehmen.

17.2.2 Die Unterrichtung des alten Arbeitgebers über die Bewerbung

In einem weiteren Fall hatte sich ein Petent bei dem Arbeitsförderbetrieb einer Stadtverwaltung um eine Stelle beworben. Da er zu diesem Zeitpunkt noch bei einer Möbelfirma beschäftigt war, bat er bei dem Vorstellungsgespräch um Vertraulichkeit, welche ihm seitens des Arbeitsförderbetriebes ausdrücklich zugesichert wurde.

Gleichwohl informierte der Arbeitsförderbetrieb die Möbelfirma über das Bewerbungsgespräch. Daraufhin wurde dem Petenten gekündigt. Der LfD beanstandete die Übermittlung durch den Arbeitsförderbetrieb als Verstoß gegen datenschutzrechtliche Vorschriften, da sie sich mit den restriktiven Bestimmungen bei der Verarbeitung von Bewerberdaten nicht vereinbaren ließ: Gemäß § 31 Abs. 1 LDSG dürfen öffentliche Stellen personenbezogene Daten von Beschäftigten nur dann verarbeiten, soweit dies zur Begründung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Nach Abs. 6 der Vorschrift dürfen personenbezogene Daten von Personen, die sich um eine Einstellung bewerben, nur übermittelt werden, soweit dies im Rahmen des Einstellungs- und Auswahlverfahrens erforderlich ist. Da hiervon bei der vorliegenden Informationsweitergabe keine Rede sein konnte und auch andere Rechtsvorschriften, auf die sich eine Übermittlung stützen würde, nicht in Betracht kamen, war diese rechtswidrig.

17.3 Auskunft an den Dienstvorgesetzten über eine nebenberufliche Tätigkeit an einer anderen Behörde

Ein Musiklehrer bat um eine Stellungnahme zu der Frage, ob die Kreisverwaltung, für die er nebenberuflich Musikunterricht gab, dem Schulleiter seiner Schule, an der er hauptberuflich tätig war, Auskunft über seine Arbeitszeiten einschließlich evtl. Fehlzeiten erteilen durfte.

Da der Betroffene bei der Kreisverwaltung auf der Basis eines Arbeitsvertrages beschäftigt war, kam § 31 LDSG zur Anwendung. § 31 Abs. 2 LDSG regelt die Übermittlung personenbezogener Beschäftigtendaten zwar nur an nichtöffentliche Stellen. Auf die Informationsweitergabe an öffentliche Stellen kann diese Vorschrift jedoch entsprechend angewandt werden.

Als Übermittlungsregelung kam § 31 Abs. 2 Ziff. 5 LDSG in Betracht, wonach eine Übermittlung von Beschäftigtendaten zulässig ist, soweit die empfangende Stelle ein rechtliches Interesse darlegt und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

Rechtliche Interessen in diesem Sinne sind solche, welche mit Hilfe der Rechtsordnung durchgesetzt und vollstreckt werden können. Demnach muss die Kenntnis der angeforderten Daten zur Geltendmachung von Rechtsansprüchen im Rahmen einer bereits bestehenden vertraglichen oder gesetzlichen Rechtsbeziehung zwischen dem Datenempfänger und dem Betroffenen erforderlich sein. Im vorliegenden Fall lagen dem Schulleiter offenbar Anhaltspunkte dafür vor, dass die in seiner Schule beschäftigte Lehrkraft während bestehender Arbeitsunfähigkeit eine Nebentätigkeit an der Kreismusikschule ausgeübt hatte. Mit der Anfrage sollten weitere Informationen hinzugewonnen werden, um feststellen zu können, ob von einem schuldhaften Fernbleiben vom Dienst ausgegangen werden konnte. Dies kann den Verlust der Bezüge, Rückforderungsansprüche des Dienstherrn oder Maßnahmen nach dem Landesdisziplinargesetz nach sich ziehen. Insgesamt lagen damit auf Seiten der datenanfordernden Schule mit Hilfe der Rechtsordnung durchsetzbare Interessen vor, die nur bei Kenntnis der angeforderten Informationen auch realisiert werden konnten.

Unter dem Gesichtspunkt der Zweckbindung hätten jedoch überwiegende schutzwürdige Interessen des Betroffenen einer Datenübermittlung entgegenstehen können. Dies wäre dann zu bejahen gewesen, wenn zugunsten des Betroffenen ein schutzwürdiges Vertrauen dahin gehend anzuerkennen wäre, dass Informationen über seine Tätigkeit an der Kreismusikschule seinem Dienstherrn nicht bekannt gegeben werden. Dies war allerdings nicht der Fall. Aufgrund der Parallelen zwischen Haupt- und nebenberuflicher Tätigkeit (in beiden Fällen Lehrtätigkeit bei einem öffentlichen Arbeitgeber) in Verbindung mit der beamtenrechtlichen Anzeigepflicht von Nebentätigkeiten konnte der Betroffenen nicht davon ausgehen, dass zwischen beiden Beschäftigungsstellen keine dienstlich relevanten Informationen ausgetauscht werden.

17.4 Aufbewahrung von Lehrerpersonalakten bei der ADD

Nachdem zum 1. Januar 2000 die Zuständigkeit für die Verarbeitung von Lehrerpersonalakten zentral auf die ADD übergegangen war, kam es im Berichtszeitraum wiederholt vor, dass bestimmte Personalakten, etwa bei der Inruhestandsversetzung eines Schulleiters, nicht aufzufinden waren.

Der LfD nahm dies zum Anlass, örtliche Feststellungen zur Personalaktenführung bei der ADD zu treffen. Diese haben ergeben, dass durch die Einführung einer neuen Registratur und eines neuen Personalverwaltungssystems zumindest künftig das Auffinden von Lehrerpersonaldaten erleichtert wird. Das Nichtauffinden bestimmter Personalakten in der Vergangenheit wurde mit den gewaltigen Datenmengen erklärt, welche nach der Zuständigkeitsverlagerung bewältigt werden mussten. So verwaltet die ADD derzeit nicht weniger als 40 000 Lehrerpersonalakten.

Die örtlichen Feststellungen haben des Weiteren ergeben, dass in Bezug auf die räumliche Absicherung insoweit Nachholbedarf bestand, als es auch Unbefugten möglich war, in die Registratur zu gelangen. Die ADD sagte jedoch zu, ein elektronisches Zugangssystem zu beschaffen, um den Zugang zu den einzelnen Räumen zu steuern, wodurch künftig der unbefugte Zugang zu geschützten Personalakten nunmehr verlässlich ausgeschlossen werden kann.

17.5 Aufzeichnung von Telefonaten in Rettungsleitstellen

Eine Rettungsleitstelle fragte an, ob bzw. in welchem Umfang und unter welchen Voraussetzungen eingehende Notrufe für arbeitsrechtliche Maßnahmen ausgewertet werden dürfen. In einem Zeitungsartikel wurde über ein angebliches Fehlverhalten eines Mitarbeiters der Rettungsleitstelle berichtet, welches zum Tod eines Menschen geführt habe. Zur Überprüfung des Vorwurfs wurde die sog. Langzeitdokumentation über den konkreten Einsatz abgehört und hierüber ein Protokoll erstellt. Wie sich herausstellte, stand in der fraglichen Zeit ein Einsatzfahrzeug nicht zur Verfügung, wodurch es zu Verzögerungen in der Versorgung des Patienten kam. Dem Mitarbeiter der Leitstelle konnte insoweit kein Vorwurf gemacht werden.

Die Aufzeichnung der eingehenden Notrufe dient der Beweissicherung und der zuverlässigen Durchführung des Einsatzes im Interesse der Hilfesuchenden. Sie ist vom Gesetzgeber zwar nicht ausdrücklich legitimiert worden; aus datenschutzrechtlicher Sicht bestehen jedoch insoweit keine Bedenken, als diese Aufzeichnungen über den allgemeinen Notstandsgedanken gerechtfertigt und damit nicht unbefugt im Sinne des § 201 StGB – Verletzung der Vertraulichkeit des Wortes – erfolgen. Hinzu kommt, dass § 31 Abs. 5 LDSG eine vergleichbare Regelung enthält. Hiernach ist die Nutzung von Protokolldaten lediglich für Zwecke einer allgemeinen Verhaltens- und Leistungskontrolle untersagt. Dem Arbeitgeber ist es daher nicht grundsätzlich verboten, Daten, welche im Rahmen der Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage anfallen, für arbeitsrechtliche oder disziplinarrechtliche Maßnahmen zu nutzen. Bei Vorliegen von Anhaltspunkten für ein pflichtwidriges Verhalten dürfen diese Daten somit ausgewertet werden. Dies hat der Gesetzgeber nunmehr ausdrücklich in der o. g. Regelung klargestellt.

Zu beachten ist jedoch die ordnungsgemäße Beteiligung der Personalvertretung. Denn die Aufzeichnung der Telefonate ist tatsächlich geeignet, die Leistungen und das Verhalten der Mitarbeiter zu überwachen und somit nach dem LPersVG mitbestimmungspflichtig. Dienststelle und Mitarbeitervertretung haben insoweit die Möglichkeit, über den Abschluss einer Dienstvereinbarung die Zulässigkeit der Auswertung von Notrufaufzeichnungen nach ihren Bedürfnissen selbst zu regeln. Hier sollte festgelegt werden, welche Personen unter welchen Voraussetzungen die aufgezeichneten Gespräche auswerten dürfen und wann diese Aufzeichnungen zu löschen sind. Die Rettungsleitstelle wurde in dem o. g. Sinne über die Rechtsauffassung des LfD unterrichtet.

17.6 Heimarbeitsplätze beim Medizinischen Dienst der Krankenversicherung

Im 18. Tb. wurde unter Tz. 17.3 über die Möglichkeiten einer pseudonymisierten Datenverarbeitung am Heimarbeitsplatz berichtet. In der Zwischenzeit wird seitens des MDK folgende Verfahrensweise praktiziert: Anstelle des Klarnamens des betroffenen Patienten werden die Namensinitialen sowie das Geburtsdatum als Zuordnungskriterium verwandt. Ein Ausdrucken der Gutachten am Heimarbeitsplatz ist nicht möglich. Seit Juni 2002 ist auch die EDV-technische Umsetzung der pseudonymisierten Datenverarbeitung am Heimarbeitsplatz realisiert.

Damit konnte in einem besonders sensiblen Bereich eine Lösung gefunden werden, welche sowohl den datenschutzrechtlichen Interessen wie auch den Interessen der MDK-Mitarbeiter gerecht wird.

18. Datenschutz im kommunalen Bereich

18.1 Datenschutzgerechtes E-Government

Das Erscheinungsbild der öffentlichen Verwaltungen wird immer mehr von dem Wunsch nach einer möglichst umfassenden und direkten Einbindung elektronischer Informations-, Kommunikations- und Transaktionsmöglichkeiten geprägt. Längst gehören z. B. die eigene Homepage oder die Nutzung internetbasierter Kommunikationsmedien zum Standard der Verwaltungen in Bund, Ländern und Gemeinden. Damit sich diese Bestrebungen, die langfristig auch die elektronische Abwicklung komplexer Dienstleistungen zum Ziel haben, erfolgreich durchsetzen können, bedarf es jedoch nicht nur der Schaffung der hierfür erforderlichen technischen Infrastruktur, sondern auch der Gewährleistung von Datenschutz und Datensicherheit. Denn nur dann, wenn alle Beteiligten davon ausgehen können, dass ihre Kommunikation mit der Verwaltung sicher und vertraulich ist und dass dabei ihre personenbezogenen Daten umfassend geschützt sind, wird auch die notwendige Akzeptanz für E-Government-Anwendungen zu erreichen sein.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aus diesem Grunde in einer Arbeitsgruppe unter Leitung des Landesbeauftragten für den Datenschutz Niedersachsen Handlungsempfehlungen für eine datenschutzgerechte Ausgestaltung von E-Government-Lösungen erarbeitet. Ziel der Ende des Jahres 2002 fertig gestellten Handreichung ist es, einerseits die Anforderungen von Datenschutz und Datensicherheit im Zusammenhang mit E-Government aufzuzeigen und darüber hinaus praktische Hinweise zu geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können. Exemplarisch aufgeführte Referenzanwendungen für bereits in der Praxis eingesetzte Verfahren zeigen, dass datenschutzfreundliche Lösungen beim E-Government möglich und wirtschaftlich zumutbar sind.

Die Handlungsempfehlungen stehen als Druckausgabe zur Verfügung und werden zudem über die Internetseiten des LfD (www.datenschutz.rlp.de) als Download angeboten.

18.2 Über allen Dächern ist Ruh' – Mobilfunkantennen

Die datenschutzrechtliche Beurteilung der Speicherung und Veröffentlichung personenbezogener Standortdaten von Mobilfunkantennen stand bereits seit Frühjahr 2002 bundesweit in der Diskussion. Mehrere Landesdatenschutzbeauftragte äußerten sich in z. T. kontroversen Stellungnahmen zu dieser Frage. Zur Erreichung einer einheitlichen Position wurde das Thema in die Tagesordnung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgenommen. In einer gemeinsamen Entschließung (vgl. Anlage 13) forderte die Konferenz den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden. Dabei solle insbesondere geregelt werden, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist.

Trotz der ausdrücklich geäußerten Absicht ist bislang seitens des Bundesgesetzgebers die geforderte gesetzliche Regelung über die Erstellung und Veröffentlichung von Mobilfunkkatastern noch nicht getroffen worden. Mangels einer bereichsspezifischen Regelung sind daher bis auf weiteres für die datenschutzrechtliche Beurteilung der Speicherung und Veröffentlichung der personenbezogenen Standortdaten die allgemeinen datenschutzrechtlichen Bestimmungen maßgebend.

Der LfD hat bezogen auf seinen Zuständigkeitsbereich eine entsprechende Orientierungshilfe (vgl. Anlage 30) veröffentlicht. Im Ergebnis hält er nach der gegenwärtigen Rechtslage – abgesehen von der datenschutzrechtlich unproblematischen Verarbeitung anonymisierter Standortdaten – zwar eine internetgestützte Veröffentlichung der personenbezogenen Informationen für unzulässig. Gegen eine lokale Verbreitung dieser Daten bestehen jedoch, zumindest, soweit es sich um sichtbare Sendeanlagen handelt, nach Auffassung des LfD keine Bedenken, so dass dem Informationsbedürfnis der direkt von den Sendeanlagen betroffenen Bevölkerung schon jetzt in weiten Teilen entsprochen werden kann.

18.3 Teilnahmerecht der Ortsbürgermeister an nichtöffentlichen Sitzungen des Verbandsgemeinderates

Im Zusammenhang mit dem in § 69 Abs. 3 GemO geregelten Teilnahmerecht der Ortsbürgermeister an Sitzungen des Verbandsgemeinderates und seiner Ausschüsse ist an den LfD die Frage herangetragen worden, ob ein Teilnahmerecht der Ortsbürgermeister auch dann gegeben sei, wenn dies eine nichtöffentliche Sitzung beträfe, in der beispielsweise Personalangelegenheiten der Verbandsgemeinde oder sonstige Inhalte zu erörtern wären, die nicht die Belange der Ortsgemeinde berühren.

Nach § 69 Abs. 3 GemO können die Ortsbürgermeister an den Sitzungen des Verbandsgemeinderates und an den Sitzungen seiner Ausschüsse, in denen Belange ihrer Ortsgemeinden berührt werden, mit beratender Stimme teilnehmen. Nach übereinstimmender Auffassung des ISM und des Gemeinde- und Städtebundes steht damit den Ortsbürgermeistern ein uneingeschränktes Teilnahmerecht bei allen Ratssitzungen der Verbandsgemeinde zu. Lediglich die Teilnahme an Ausschusssitzungen beschränke sich auf solche, in denen Belange der Ortsgemeinde berührt werden.

Aus datenschutzrechtlicher Sicht bestehen Zweifel, ob eine Teilnahme der Ortsbürgermeister an den nichtöffentlichen Sitzungen des Verbandsgemeinderates auch dann gerechtfertigt ist, wenn die Belange ihrer Gemeinden nicht berührt werden. Denn in diesem Fall besteht gerade aus materiellen Gründen keine Notwendigkeit für ein Mitwirkungs- und Teilnahmerecht der Ortsbürgermeis-

ter, zumal dies im Zusammenhang mit Ausschusssitzungen unumstritten ist. Da jedoch in der kommunalen Praxis das Teilnahmerecht der Ortsbürgermeister weder nach Kenntnis des LfD noch des Gemeinde- und Städtebundes bislang zu datenschutzrechtlichen Problemen geführt hat und darüber hinaus die Ortsbürgermeister der Schweigepflicht des § 20 GemO unterliegen, wurde davon abgesehen, die genannten Zweifel an der Gesetzesauslegung gegenüber dem ISM weiter zu thematisieren.

18.4 Aufdringliche Überzeugungsarbeit

Nachdem im Rat einer Ortsgemeinde die Aufgabe des alten gemeindeeigenen Sportgeländes sowie die Neuerrichtung einer Sportanlage an anderer Stelle beschlossen wurde, bildete sich eine Bürgerinitiative zum Erhalt der bisherigen Sportstätte und begründete durch Sammlung einer ausreichenden Zahl von Unterschriften ein Bürgerbegehren im Sinne von § 17 a GemO. Nach Zurückweisung des Bürgerbegehrens durch den Rat kam es zur Durchführung eines Bürgerentscheides. In dessen Vorfeld wandte sich der Ortsbürgermeister unter Verwendung der in den Unterschriftenlisten enthaltenen Bürgerdaten (Personalien und Anschriften) mit einem persönlichen Anschreiben in Form eines Serienbriefes und einer Broschüre an die Unterstützer des Bürgerbegehrens, um diese zu einer Änderung ihrer bisherigen Meinung zu bewegen. Eine Einwilligung der Betroffenen hierzu lag nicht vor.

Datenschutzrechtlich ist zwischen der Nutzung der aus den Unterschriftenlisten stammenden Bürgerdaten und der Speicherung der Adressdaten zu unterscheiden.

Nach § 17 a Abs. 3 Satz 4 i. V. m. Abs. 4 Satz 3 GemO dienen die in den Unterschriftenlisten erhobenen Bürgerdaten (Name und Anschrift) der gesetzlich vorgesehenen Überprüfung der Gültigkeit der das Bürgerbegehren unterstützenden Eintragungen. Findet das Bürgerbegehren in einer Ortsgemeinde statt, ist diese Aufgabe der Verbandsgemeindeverwaltung zugewiesen. Die Verwendung der in den Unterschriftenlisten enthaltenen Adressdaten für ein gezieltes Anschreiben der Unterstützer des Bürgerbegehrens durch den Ortsbürgermeister stellt dagegen eindeutig eine von dem ursprünglichen Erhebungszweck abweichende Datennutzung dar. Ob angesichts der Nr. 6 der VV zu §17 a GemO i. V. m. Nr. 4 der VV zu § 17 GemO, wonach ausdrücklich eine zweckwidrige Verwendung der Unterschriftenlisten auszuschließen ist, noch Raum für eine Heranziehung der in § 5 Abs. 1 LDSG enthaltenen Voraussetzungen ist, kann dahingestellt bleiben, da im konkreten Fall weder die Einwilligung der Betroffenen noch eine entsprechende Erlaubnisvorschrift im Sinne von § 5 Abs. 1 Nr. 2 LDSG vorlagen. Die Datennutzung war folglich unzulässig.

Aus den gleichen Gründen wie die Nutzung musste auch die Speicherung der den Unterschriftenlisten entnommenen Bürgerdaten in einer gesonderten Datei mangels einer entsprechenden Rechtsgrundlage als datenschutzrechtlich unzulässig gerügt werden.

18.5 Das Weingut im Amtsblatt

Die Ausweisung eines Baugebietes in einer weinbaubetreibenden Ortsgemeinde stieß nicht bei allen Dorfbewohnern auf die gewünschte Zustimmung. Im Gegenteil, der Inhaber eines der beiden an das Baugebiet angrenzenden Weingüter stellte beim OVG einen Antrag auf Durchführung eines Normenkontrollverfahrens. Zur Unterrichtung der Öffentlichkeit über den aktuellen Verfahrensstand verfasste der Ortsbürgermeister daraufhin eine Kurznachricht, die in der nächsten Ausgabe des Amtsblattes der Verbandsgemeinde im amtlichen Teil unter der Rubrik der Ortsgemeinde abgedruckt wurde und folgenden Wortlaut hatte:

„Nachdem es schon öfters Nachfragen gab, möchte ich an dieser Stelle den aktuellen Sachstand bekannt machen. Der Bebauungsplan ist mittlerweile rechtskräftig. Jedoch hat ein im Außenbereich angrenzendes Weingut beim Oberverwaltungsgericht ein Normenkontrollverfahren beantragt. Welche zeitliche Verzögerung das wieder bedeutet, kann im Moment noch nicht gesagt werden.“

Zunächst war festzustellen, dass es sich bei dem im Text enthaltenen Hinweis um ein personenbezogenes Datum im Sinne von § 3 Abs. 1 LDSG handelte. Denn unabhängig davon, ob dieses Qualifikationsmerkmal auf ein oder zwei Weingüter zutraf, wurde mit dieser Angabe der Kreis der in Frage kommenden Antragsteller derart beschränkt, dass der tatsächliche Antragsteller mit nur noch äußerst geringem Zusatzaufwand bestimmbar war.

Im Ergebnis stellte die Bezeichnung des antragstellenden Weingutes einen Verstoß gegen das in den §§ 30 VwVfG, 1 LVwVfG enthaltene Geheimhaltungsgebot dar. Denn im Zusammenhang mit der Bekanntgabe der Beteiligtenfunktion einer Person bei Verwaltungs- bzw. verwaltungsgerichtlichen Verfahren ist das in § 30 VwVfG enthaltene und generell anzuwendende Geheimhaltungsgebot zu beachten. Danach dürfen grundsätzlich die persönlichen Tatsachen und Umstände der Betroffenen („Geheimnisse“) nicht unbefugt offenbart werden. Der Begriff des Geheimnisses ist in diesem Zusammenhang weit auszulegen und umfasst auch die Eigenschaft als Beteiligter/Antragsteller an einem Verwaltungs- bzw. verwaltungsgerichtlichen Verfahren (vgl. Kopp/Ramsauer, Kommentar zum VwVfG, Rdnr. 8 zu § 30).

Eine Befugnisnorm, nach der die Person des Antragstellers des in dem Amtsblatt konkret bezeichneten Normenkontrollverfahrens offenbart werden durfte, war nicht ersichtlich. Insbesondere konnte nicht die in § 15 Abs. 1 GemO enthaltene allgemeine Unterrichtungspflicht der Kommunen hierfür herangezogen werden. Denn diese umfasst nur wichtige Angelegenheiten der örtlichen Verwaltung. Während der derzeitige Stand bei der Erschließung von gemeindlichem Bauland durchaus als wichtige Angelegenheit i. S. v. § 15 Abs. 1 GemO qualifiziert werden muss, ist für die Umsetzung dieser Unterrichtungspflicht die Bekanntgabe von Personen, die an in diesem Zusammenhang maßgeblichen Verfahren beteiligt sind, nicht erforderlich. Eine Bezeichnung des konkreten Verfahrensstandes hätte daher zur Information der Bürger ausgereicht.

18.6 Bestellung eines behördlichen Datenschutzbeauftragten

Immer wieder wirft die Bestellung von Personen als behördlicher Datenschutzbeauftragter bei den Verwaltungen Fragen auf. So wandte sich im Berichtszeitraum der Personalrat einer Stadtverwaltung mit folgendem Anliegen an den LfD:

Im Rahmen von Verhandlungen zwischen dem Personalrat und der Stadtverwaltung über den Abschluss einer Dienstvereinbarung zur Nutzung des Internets bzw. Intranets werde die Verwaltung von einem Mitarbeiter vertreten, der zugleich die Funktion des behördlichen Datenschutzbeauftragten ausübe. Der Personalrat befürchtete, dass dieser bei der Prüfung der hierbei auftretenden datenschutzrechtlichen Fragen befangen sei und bat den LfD um seine Einschätzung.

Ob der behördliche Datenschutzbeauftragte der betroffenen Stadtverwaltung die erforderliche Zuverlässigkeit im Sinne von § 11 Abs. 1 Satz 3 LDSG besaß, konnte der LfD auf der Grundlage der vorgelegten Informationen nicht klären. Allerdings wurde die Stadtverwaltung auf die in diesem Zusammenhang maßgeblichen Gesichtspunkte hingewiesen.

Gesetzliche Grundlage für die Bestellung des behördlichen Datenschutzbeauftragten ist § 11 LDSG. Gemäß Abs. 1 Satz 3 dieser Regelung darf hierzu nur bestellt werden, „wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt“. Nach der Gesetzesbegründung ist im Rahmen der Zuverlässigkeit des behördlichen Datenschutzbeauftragten sicherzustellen, dass mit dieser Funktion nur solche Bedienstete betraut werden, die dadurch nicht in einen Interessenwiderstreit mit ihren regelmäßig wahrzunehmenden sonstigen Aufgaben geraten.

Ob Interessenkonflikte tatsächlich zu befürchten sind, kann nur mit Kenntnis der besonderen Gegebenheiten in der datenverarbeitenden Stelle beurteilt werden. Grundsätzlich sind aber Stellung und Funktion des Bediensteten Merkmale, die einen solchen Interessenkonflikt eher wahrscheinlich oder eher unwahrscheinlich erscheinen lassen. So wird in der datenschutzrechtlichen Literatur beispielsweise von der Heranziehung der Behördenleiter und ähnlich einflussreichen Bediensteten (vgl. Nungesser, Kommentar zum Hessischen Datenschutzgesetz, Anm. 11 zu § 5 HDSG), Mitarbeitern aus dem Bereich der Organisationsverwaltung (vgl. Globig/Schuber, Kommentar zum LDSG R-P, Nr. 2.5 zu § 11 LDSG) sowie EDV-Verantwortlichen (vgl. Globig/Schuber, a. a. O.; Büermann, Kommentar zum LDSG R-P, Anm. 12 zu § 11 LDSG) abgeraten. Umstritten ist die Bestellung von Mitarbeitern aus dem Personalbereich (dafür: Globig/Schuber, a. a. O.; dagegen: Büermann, a. a. O; Bergmann/Möhrle/Herb, Kommentar zum BDSG, Anm. 58 zu § 36 BDSG). In der Vergangenheit hat der LfD auf der Grundlage des § 11 Abs. 1 LDSG die Bestellung von Hauptamtsleitern zu behördlichen Datenschutzbeauftragten grundsätzlich toleriert. Auf der anderen Seite widersprach nach Auffassung des LfD die Berufung von Systemadministratoren den gesetzlichen Vorgaben des § 11 Abs. 1 LDSG.

Allgemeine Hinweise zu Stellung, Aufgaben und Befugnissen des behördlichen Datenschutzbeauftragten stehen im Internet-Angebot des LfD (www.datenschutz.rlp.de) zur Verfügung.

19. Telekommunikation

19.1 Datenschutzrichtlinie für elektronische Kommunikation verabschiedet

Im 18. Tb. (Tz. 19.3) hat der LfD über Aktivitäten des EG-Gesetzgebers berichtet, eine neue Richtlinie zum Datenschutz bei der elektronischen Kommunikation zu erlassen. Am 31. Juli 2002 ist die „Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ in Kraft getreten. Sie ersetzt die Telekommunikations-Datenschutzrichtlinie 97/66/EG aus dem Jahre 1997. Der Anwendungsbereich der neuen Richtlinie wurde erheblich ausgedehnt und bezieht sich nunmehr allgemein auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation. So soll der Schutz der Nutzerdaten unabhängig von der benutzten Technologie sichergestellt werden. Für die Umsetzung der Bestimmungen ist eine Frist bis zum 31. Oktober 2003 vorgesehen. Davon betroffen sind die Datenschutzvorschriften in den Bereichen Telekommunikation und Multimedia. Zu der wünschenswerten einheitlichen Regelung von Telekommunikations- und Telediensten in einem Regelwerk wird es nach dem gegenwärtigen gesetzgeberischen Ansatz nicht kommen. Das BMWA bereitet parallel zur TKG-Novelle (vgl. Tz. 19.2) eine Neuordnung des Datenschutzes in elektronischen Medien (vgl. Tz. 20.1) vor.

Die Richtlinie stärkt in weiten Teilen die Rechte des Nutzers von elektronischen Kommunikationsnetzen. So ist die Regelung über unerbetene Nachrichten, die sich bisher nur auf automatische Anrufsysteme und Faxgeräte für Zwecke der Direktwerbung bezog, auf elektronische Post ausgeweitet worden. Nach Art. 13 Abs. 1 darf elektronische Post nicht für Zwecke der Direktwerbung verwendet werden, wenn keine vorherige Einwilligung der Teilnehmer vorliegt. Damit hat sich grundsätzlich das Opt-in-Modell (vgl. dazu Tz. 20.3) durchgesetzt. Eine Einschränkung erfährt diese Regelung dann, wenn bereits ein Kontakt zu einem Kunden besteht. In diesen Fällen gilt eine Opt-out-Regelung, was bedeutet, dass Werbesendungen per E-Mail zunächst gestattet sind. Widerspricht der Kunde jedoch einer solchen Werbung, so hat sie künftig zu unterbleiben. Die Kunden sind auf das Widerspruchsrecht hinzuweisen. Ausdrücklich verboten ist die Versendung von Werbe-E-Mails ohne Angabe des Absenders (Art. 13 Abs. 4).

Neu aufgenommen wurde eine Regelung zu Standortdaten im Mobilfunk, die nur unter bestimmten Voraussetzungen verarbeitet und an Dritte übermittelt werden dürfen. Damit sollte eine Schutzvorschrift zugunsten der Nutzer so genannter standortbasierter Dienste (Location Based Services [vgl. Tz. 19.2]) geschaffen werden.

In dem Verfahren zum Erlass der Richtlinie war die Regelung in Art. 15 Abs. 1 zwischen dem Rat der Europäischen Union und dem Europäischen Parlament umstritten, wonach es grundsätzlich gestattet ist, Vorschriften zur Vorratsdatenspeicherung (vgl. dazu allgemein Tz. 19.3) zu erlassen. So ermöglicht eine Öffnungsklausel es den Mitgliedstaaten, für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, Beschränkungen der Schutzvorschriften der Richtlinie zur Vertraulichkeit, der Verarbeitung von Verkehrsdaten, der Rechte der Nutzer im Hinblick auf die Rufnummernanzeige sowie die Verarbeitung von Standortdaten zu erlassen. Die Mitgliedstaaten können nach Art. 15 Abs. 1 durch Rechtsvorschriften vorsehen, dass die genannten Daten während einer begrenzten Zeit aufbewahrt werden. Die Maßnahmen müssen im Einklang mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgen und „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ sein (vgl. hierzu Erwägungsgrund 11). Es ist darauf hinzuweisen, dass die Bestimmung des Art. 15 Abs. 1 der Richtlinie keine Verpflichtung der Mitgliedstaaten zum Erlass von Rechtsvorschriften zur Vorratsdatenspeicherung in den vorgenannten Grenzen darstellt, sondern diese lediglich ermöglicht.

19.2 Novellierung des Telekommunikationsgesetzes

Die Datenschutzvorschriften im Bereich Telekommunikation müssen aufgrund der umzusetzenden Datenschutzrichtlinie für elektronische Kommunikation angepasst werden. Nach dem vorliegenden Referentenentwurf (Stand: 30. April 2003) plant das BMWA unter Auflösung der Telekommunikations-Datenschutzverordnung (vgl. 18. Tb., Tz. 19.1) einen eigenen Abschnitt „Datenschutz“ und einen sich hieran anschließenden Teil „Fernmeldegeheimnis, öffentliche Sicherheit“ im Telekommunikationsgesetz.

Es ist u. a. vorgesehen, dass Unternehmen, die ihren Mitarbeitern die Privatnutzung ihrer Kommunikationseinrichtungen gestatten, auch weiterhin als geschäftsmäßige Anbieter von Telekommunikationsdiensten Normadressaten sein werden. Dementsprechend bleiben sie für Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten verantwortlich. Des Weiteren ist eine Regelung zu sog. Standortdaten enthalten. Dies ist insbesondere im Zusammenhang mit der Nutzung von sog. „Location Based Services“ von Bedeutung. Hierbei handelt es sich um standortbezogene Dienste, wobei die Dienstleistungen und Serviceangebote dem Nutzer in Abhängigkeit von seinem Standort zur Verfügung gestellt werden. Beispiele sind etwa Hinweise auf Restaurants, Kinos oder Verkehrsinformationen. Hier besteht die Gefahr des „gläsernen“ Mobilfunknutzers, dessen Bewegungsprofile erfasst werden können. Ferner könnten Nutzerprofile erstellt werden, die Aufschluss über den persönlichen Lebensstil oder das Kaufverhalten geben. Notwendige Voraussetzung für die Übermittlung und Nutzung von Standortdaten soll nach dem Entwurf nun regelmäßig das Vorliegen einer informierten Einwilligung sein. Dies ist ausdrücklich zu begrüßen. Der TKG-Entwurf enthält aber auch Regelungen, die zu einer Verschlechterung des Datenschutzes führen würden. Die Kritikpunkte haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation“ (vgl. Anlage 22) angesprochen.

Zwischenzeitlich hat das BMWA einen neuen Referentenentwurf zur Ressortabstimmung vorgelegt, der jedoch den Landesdatenschutzbeauftragten bislang (Stand: 30. September 2003) nicht zugänglich gemacht wurde. In diesem Zusammenhang steht zu befürchten, dass der neue Entwurf aus datenschutzrechtlicher Sicht wiederum Verschlechterungen enthalten wird (u. a. die Speicherung vollständiger Zielrufnummern für sechs Monate nach Versand der Rechnung als Regelfall). Der weitere Verlauf des Gesetzgebungsverfahrens bleibt also abzuwarten. Mit einer fristgerechten Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation bis zum 31. Oktober 2003 ist jedenfalls nicht mehr zu rechnen. Sobald der bislang interne Entwurf zugänglich sein wird und sich ihre Befürchtungen bestätigen, erwägen die Datenschutzbeauftragten im Wege einer Entschließung, die Öffentlichkeit zeitnah über die geplanten datenschutzrechtlichen Verschlechterungen zu informieren.

19.3 Pläne zur Vorratsdatenspeicherung

Der Bundesrat beschloss mit knapper Mehrheit einen Gesetzentwurf, mit dem u. a. sämtliche Anbieter von Telekommunikations- und Telediensten verpflichtet werden sollten, die bei ihnen anfallenden Verbindungs- und Nutzungsdaten für Zwecke der Strafverfolgung, der Sicherheitsbehörden und Nachrichtendienste ohne Anlass für eine bestimmte Mindestfrist zu speichern. Hier wurden wesentliche datenschutzrechtliche Grundsätze außer Acht gelassen. Dieser Gesetzentwurf war aus Datenschutzsicht als ein massiver Angriff auf das Recht auf informationelle Selbstbestimmung zu werten.

Zuvor hatte der LfD die Staatskanzlei, das Innenministerium, das Justizministerium und das Wirtschaftsministerium auf die Bundesratsinitiative hingewiesen und darum gebeten, bei der Abstimmung im Bundesrat am 31. Mai 2002 den Empfehlungen des Rechtsausschusses des Bundesrates nicht zu folgen, was dann auch geschehen ist. In diesem Zusammenhang hat sich das Ministerium der Justiz in einer Pressemitteilung vehement gegen die Gesetzesinitiative des Bundesrates ausgesprochen. So sei die Kritik zahlreicher

Datenschützer, Deutschland werde zum unrühmlichen Vorreiter bei der totalen Überwachung der Informationsgesellschaft, leider begründet. Selbstverständlich dürfe und müsse der Staat zur Verhinderung und Aufklärung von Straftaten erforderliche Daten sammeln. Das sei auch bereits zulässig. Wenn aber ohne jeden Verdacht wahllos alle verfügbaren Daten über unbescholtene Bürger gespeichert würden, gehe das entschieden zu weit. Die grenzenlose Datensammelwut führe überdies dazu, dass die Strafverfolgungsbehörden irgendwann im Datenmüll ersticken würden. Einer effektiven Kriminalitätsbekämpfung würde damit ein Bärendienst erwiesen.

Des Weiteren bekräftigte die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Oktober 2002 ihre Auffassung, dass eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallenden Daten auf Vorrat mit dem deutschen Verfassungsrecht nicht zu vereinbaren ist (vgl. Anlage 12). Bereits die 63. Konferenz vom 7. März 2002 wies in einer Entschließung (vgl. Anlage 8) darauf hin, dass nach dem geltenden Recht Anbieter von Tele-, Medien- und Telekommunikationsdiensten weder berechtigt noch verpflichtet sind, generell Daten auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke benötigen. Schließlich hat auch die Konferenz der Europäischen Datenschutzbeauftragten in einer Erklärung vom 11. September 2002 gravierende Zweifel hinsichtlich der Legitimität von weit reichenden Maßnahmen zur Vorratsdatenspeicherung angemeldet und unter Bezugnahme auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte betont, dass eine solche Datenspeicherung auf Vorrat ein unzulässiger Eingriff in die Grundrechte des Einzelnen nach Art. 8 EMRK sei (vgl. Anlage 35). Die Art. 29-Datenschutzgruppe (vgl. Tz. 3.4) hat sich am 11. Oktober 2002 in einer Stellungnahme der Erklärung der Europäischen Datenschutzbeauftragten angeschlossen.

Zwar hat der Deutsche Bundestag über den Gesetzentwurf des Bundesrates in der vergangenen Legislaturperiode nicht mehr entschieden. Dennoch gibt es sowohl auf nationaler als auch auf europäischer Ebene nach wie vor starke Bestrebungen, die Anbieter zu einer Datenspeicherung auf Vorrat zu verpflichten. Der LfD wird diesen Überlegungen auch künftig entschieden entgegentreten.

19.4 Identifikationszwang beim Erwerb eines „vertragslosen“ Handys

Im März 2002 veröffentlichte die Bundesregierung „Eckpunkte zur Anpassung der Regelung des § 90 Telekommunikationsgesetz“. Darin wurde die Absicht bekundet, alle Anbieter von Telekommunikationsdienstleistungen zu verpflichten, Namen, Anschriften und Geburtsdaten jedes Kunden durch Vorlage des Personalausweises zu erfassen, und zwar unabhängig davon, ob sie die Daten für die Vertragsabwicklung benötigen. Zur Begründung wurde ausgeführt, die Verwendung anonym oder pseudonym erworbener „Prepaid-Karten“ erschwere die Ermittlungstätigkeit der Sicherheitsbehörden. Die Unternehmen selbst haben an dieser Datenverarbeitung kein Interesse. Sie würden es vorziehen, ihre entsprechenden Produkte z. B. in Kaufhäusern ohne Formalitäten vertreiben zu können. So sind auch erfahrungsgemäß die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch. Zur Erläuterung sei ausgeführt, dass es sich bei dem Begriff der „erworbenen Prepaid-Karte“ um die i. d. R. beim Erwerb eines „vertragslosen“ Handys mitgelieferte bzw. auch einzeln beziehbare, im Prepaid-Verfahren mit Guthaben aufladbare „SIM-Karte“ handelt.

Dem Vorhaben der Bundesregierung ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 24. Mai 2002 zum geplanten Identifikationszwang in der Telekommunikation entschieden entgegengetreten. Die Konferenz hat insbesondere auf Folgendes hingewiesen: Durch die geplante Gesetzesänderung wird nicht verhindert, dass Straftäter bewusst und gezielt in kurzen Abständen neue Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig wechseln oder untereinander austauschen. In der Begründung ist auch nicht plausibel dargelegt, dass die Ermittlungstätigkeit durch die geplante Änderung tatsächlich erleichtert wird. Darüber hinaus wird die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, konterkariert. Gerade das Prepaid-Verfahren ist ein gutes Beispiel für den Einsatz datenschutzfreundlicher Technologien, da es anonymes Kommunizieren auf unkomplizierte Weise ermöglicht. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

Die Frage des hier beschriebenen Identifikationszwangs bleibt auf der Tagesordnung: So wird das Vorhaben im Rahmen der anstehenden Novellierung des Telekommunikationsgesetzes (siehe Tz. 9.2) weiter betrieben (vgl. § 106 TKG-E vom 30. April 2003).

20. Medien

20.1 Fortentwicklung der Medienordnung

Der Schutz personenbezogener Daten der Nutzer von elektronischen Medien ist gegenwärtig in verschiedenen – inhaltlich jedoch weitgehend einheitlichen – Regelwerken in Bund und Ländern enthalten. Für den Bereich der Tele- und Mediendienste wurden 1997 die spezifischen Datenschutzbestimmungen im geltenden Teledienstedatenschutzgesetz und im Mediendienste-Staatsvertrag der Länder geschaffen. Ebenso enthält der Rundfunkstaatsvertrag der Länder vergleichbare Datenschutzbestimmungen. Aufgrund der Erfahrungen und Entwicklungen im Bereich der IuK-Dienste bestand Änderungs- und Modernisierungsbedarf bei den Bestimmungen, die mit einer entsprechenden Änderung des Teledienstedatenschutzgesetzes (vgl. 18. Tb., Tz. 20.1) sowie Änderungen der Datenschutzbestimmungen im Mediendienste-Staatsvertrag umgesetzt wurden.

Der Datenschutz in den elektronischen Medien soll nun in Zukunft einheitlich durch den Bund geregelt werden. Hierzu ist ein neues Gesetz über den Datenschutz in elektronischen Medien (EMDSG) vorgesehen, das auf den geltenden Bestimmungen in Bund und Ländern aufbaut und diese ersetzt. Ziel ist es, durch die Zusammenführung der Bereiche Teledienste, Mediendienste und Rundfunk in ein Gesetz das Datenschutzrecht für die elektronischen Medien zu vereinfachen. Insbesondere begrüßenswert ist die Klärung der alten Streitfrage „Telekommunikations- oder Teledienst“ durch die geplante explizite Zuordnung der Zugangsvermittlung, der E-Mail-Dienste und der Internettelefonie zu den Telekommunikationsdiensten. Hier wird also hinsichtlich der Datenschutzrichtlinie für elektronische Kommunikation (vgl. Tz. 19.1) klargestellt, dass Kommunikationsdienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, nicht unter das EMDSG fallen.

Auf der Ebene der Länder wurde die geplante Neuordnung u. a. in der Arbeitsgruppe „Datenschutz“ der Rundfunkreferenten der Länder beraten mit dem Ziel, gemeinsam mit den Aufsichtsbehörden für den Datenschutz sowie den Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten zu einer einheitlichen Auffassung auf Länderseite zu gelangen.

Im Mai 2003 hat das BMWA Änderungsvorschläge zum ursprünglichen EMDSG-Entwurf vom 6. November 2002 unterbreitet. Daraus ergibt sich u. a., dass nunmehr die ursprünglich beabsichtigte Neuordnung der Aufsichtsstruktur nicht mehr weiter verfolgt wird. Die daraufhin geplante Bund-Länder-Besprechung hat aus terminlichen Gründen nicht stattgefunden. Seit Mai 2003 hat es daher keinen sichtbaren Fortgang der Angelegenheit mehr gegeben. Dem Vernehmen nach beabsichtigt das BMWA, bis Ende 2003 ein Eckpunktepapier zur Medienordnung zu entwerfen, auf dessen Grundlage dann ein neuer Gesetzentwurf vorgelegt werden soll. Da die Länder die Kompetenz über den Rundfunk haben, wird darauf zu achten sein, dass die Fortentwicklung der Medienordnung verfassungskonform betrieben wird.

20.2 Anpassung des Pressegesetzes

Eine Neuregelung für den Redaktionsdatenschutz ist notwendig geworden, nachdem die Europäische Union eine Datenschutzrichtlinie (vgl. Tz. 3.1) formuliert und damit auch die Basis für ein neues Bundesdatenschutzgesetz gelegt hatte. Nach § 41 Abs. 1 BDSG haben die Länder in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38 a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen. Das BDSG enthält damit insoweit für die Presse und ihre Hilfsunternehmen nur wenige Vorschriften. Dies sind insbesondere die Verpflichtung zur Wahrung des Datengeheimnisses (§ 5 BDSG) sowie die Vorgaben zu den technischen und organisatorischen Maßnahmen (§ 9 BDSG). Außerdem wird auf ein Instrument verwiesen, das durch die Europäische Datenschutzrichtlinie neu eingeführt wurde: nämlich die Möglichkeit, dass die beteiligten Verbände selbst für ihre Mitgliedsunternehmen bestimmte Vorgaben für den Datenschutz aufstellen (§ 38 a BDSG, verbandsrechtliche Selbstregulierung).

§ 41 Abs. 1 BDSG enthält also inhaltlich ein „Medienprivileg“, kompetenzrechtlich eine Rahmenvorschrift des Bundesgesetzgebers. Somit sind sämtliche 16 Bundesländer gehalten, diese Regelung auf Landesebene umzusetzen. Die Bundesländer bedienen sich hierbei der Landespressegesetze, wobei die meisten Regelungen auf eine dynamische Verweisung der Landesgesetze auf das Bundesdatenschutzgesetz hinauslaufen. In Rheinland-Pfalz wurden die in § 41 Abs. 1 BDSG für die Presse und deren Hilfsunternehmen getroffenen rahmenrechtlichen Regelungen inhaltlich unverändert übernommen, um damit die Voraussetzung zu schaffen, dass für die Presse in der Bundesrepublik Deutschland möglichst einheitliche datenschutzrechtliche Anforderungen gelten. Es wäre aus Sicht des LfD auch äußerst problematisch, wenn für die vielfach überregional tätige Presse, bezogen auf die einzelnen Bundesländer, unterschiedliche datenschutzrechtliche Vorgaben zu beachten wären.

Auf dieser Grundlage hat der Deutsche Presserat seine Tätigkeit zur Einhaltung des Redaktionsdatenschutzes ausgeweitet. Inhalt der Selbstregulierung sind insbesondere die Erarbeitung von Verhaltensregeln und Empfehlungen, eine regelmäßige Berichterstattung zum redaktionellen Datenschutz sowie die Schaffung eines Beschwerdeverfahrens, das Betroffenen die Möglichkeit einer presseinternen Überprüfung beim Umgang mit personenbezogenen Daten eröffnet. Der Pressekodex stellt bereits in seiner Präambel klar, dass „von der Recherche über die Radaktion, Veröffentlichung, Dokumentation bis hin zur Archivierung dieser Daten die Presse das Privatleben, die Intimsphäre und das Recht auf informationelle Selbstbestimmung des Menschen“ achtet. Des Weiteren reagiert

der Deutsche Presserat im Bereich des Redaktionsdatenschutzes nicht nur anlassbezogen auf konkrete Beschwerden, sondern wird daneben auch präventiv tätig. Hierzu gehört die Entwicklung von Verhaltensregeln und Empfehlungen für den Umgang mit personenbezogenen Daten in den Redaktionen. Der Presserat hat auch ein Konzept zur Datensicherheit in Form eines Präventionskatalogs erarbeitet. Darüber hinaus wird er die Verlage und Redaktionen zum Thema Redaktionsdatenschutz beraten und regelmäßig alle zwei Jahre über die aktuelle Situation des Datenschutzes in den Redaktionen öffentlich berichten. Es wurde ein besonderer Beschwerdeausschuss gegründet, der aus sechs Personen besteht. Nach der Beschwerdeordnung des Presserates ist jeder berechtigt, sich bei diesem über Veröffentlichungen oder Vorgänge zu beschweren. Dies kommt insbesondere dann in Betracht, wenn jemand der Auffassung ist, dass die Verarbeitung von personenbezogenen Daten zu journalistisch-redaktionellen Zwecken im Rahmen der Recherche oder Veröffentlichung das Recht auf Datenschutz verletzt. Der Beschwerdeausschuss kann, falls eine Beschwerde begründet ist, einen Hinweis, eine Missbilligung oder eine Rüge aussprechen. Kommt es zu einer Rüge, so muss diese nach den Statuten des Presserates von dem betroffenen Presseorgan veröffentlicht werden.

Für die Zukunft bleibt abzuwarten, wie sich das Konzept bewährt. Insbesondere wird die Entwicklung der Regelung zu beobachten sein, dass die Selbstregulierung nur für diejenigen Unternehmen gilt, die dem Deutschen Presserat angehören bzw. sich zur Einhaltung des Pressekodex und der Beschwerdeordnung verpflichten. Im Zusammenhang mit der auf Bundesebene anstehenden umfänglichen Modernisierung des Datenschutzrechts würde es sich anbieten, die gewonnenen Erkenntnisse dort einfließen zu lassen. Im Hinblick auf die grundrechtlich garantierte Pressefreiheit nach Art. 5 GG und die Rechtsprechung des Bundesverfassungsgerichts hierzu wird es für diesen Bereich stets darauf ankommen, bereichsspezifische Regelungen für die journalistisch-redaktionelle Arbeit sicherzustellen. Aus der Staatsferne der Medien als Verfassungsprinzip ergeben sich zusätzliche Einschränkungen staatlicher Aktivitäten. Dieser Grundsatz gilt für die Presse gleichermaßen. Es wäre aus Sicht des LfD damit unvereinbar, staatlichen Datenschutzbehörden Zuständigkeiten im Bereich der Presse einzuräumen.

Auf diese Gesichtspunkte hat der LfD auch auf dem Deutschen Juristentag in Berlin und in der von ihm – seitens des Hessischen Landtags – erbetenen Stellungnahme anlässlich der Anhörung zum Entwurf des Hessischen Pressegesetzes hingewiesen.

20.3 Betrieb eines Newsletter-Dienstes

Seitens eines Abgeordneten wurden verschiedene Fragen zum Betrieb eines so genannten Newsletter-Service an den LfD herangetragen. Es geht hierbei um die Möglichkeit, anstelle des herkömmlichen Postversandes die neuen Medien zu nutzen – beispielsweise zum Zwecke der Darstellung von Wahlkreisarbeit, Hinweise auf Termine für Bürgergespräche oder Informationen bezüglich der im Parlament gehaltenen Reden, Angebote zu Informationsfahrten usw.

Von der Konzeption her hatte der Abgeordnete vorgesehen, dass der Eintrag in die entsprechende Interessentenliste zum einen persönlich unter Nennung der eigenen E-Mail-Adresse erfolgen kann. Es sollten aber auch all jene als potentielle Informationsempfänger einbezogen werden, die im Internet ihre E-Mail-Adressen explizit auflisten.

Bezeichnen könnte man dies als die moderne Variante der Postwurfsendung: Man erhält Werbung bzw. eine Information, ohne dass man sie jemals angefordert hat oder überhaupt haben möchte.

Als Korrektiv war hier vorgesehen, dass die Angeschriebenen stets am Ende des elektronischen Briefes einen Hinweis darauf finden, wie sie den Bezug künftig stoppen können.

In diesem Zusammenhang tauchen immer wieder zwei neudeutsche Begriffe auf, nämlich das „Opt-in-“ und das „Opt-out-Verfahren“.

Das Opt-in-Verfahren sieht vor, dass der Nutzer sein ausdrückliches Einverständnis geben muss, wenn er Werbemails erhalten möchte. Er kann selbstbestimmt entscheiden, wer seine Mail-Adresse zu welchem Zweck nutzen darf. Hier ist also sozusagen die Kommunikation vom Nutzer her ausdrücklich erbeten.

Dagegen bedeutet das Opt-out-Verfahren, dass sich der Internetnutzer zur Vermeidung weiterer Werbemails in sog. Opt-out-Listen austragen muss.

Dahinter stehen zwei bekannte Modelle. Das Opt-out-Verfahren ist vergleichbar mit der Widerspruchslösung, das Opt-in-Verfahren entspricht der Einwilligungslösung.

Der LfD hat in Abstimmung mit der Landtagsverwaltung dem Abgeordneten mitgeteilt, dass es nach der gegenwärtigen Rechtslage keinen gesetzlichen Hinderungsgrund gibt, das gerade beschriebene „Opt-out-Verfahren“, also die Widerspruchslösung, beizubehalten.

Die Rechtsprechung hat sich zwar schon mehrfach mit dem Problembereich der unverlangt zugesandten Werbemails befasst und in aller Regel den Schutz der Privatsphäre der Internetnutzer sehr hoch bewertet. Eine Grundsatzentscheidung des BGH ist bislang allerdings noch nicht ergangen.

Diese Rechtslage wird jedoch demnächst modifiziert werden aufgrund der bis zum 31. Oktober 2003 umzusetzenden EG-Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (vgl. Tz. 19.1). Dort ist in Artikel 13 vorgesehen, dass die Verwendung von elektronischer Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf, also das „Opt-in-Verfahren“ (das Einwilligungsmodell) festgeschrieben. Nur wenn bereits ein Kontakt zum Empfänger besteht, ist das „Opt-out-Verfahren“ (Widerspruchsmodell) gestattet.

Aus der Entstehungsgeschichte der Richtlinie und den Erwägungsgründen lässt sich entnehmen, dass von politischen oder wohltätigen Organisationen durchgeführte Direktwerbung, z. B. Anwerbung neuer Mitglieder oder Aufrufe zur Wahlunterstützung, unter den Begriff der Direktwerbung fallen werden (also die Einwilligung erforderlich sein wird). Nachrichten zu anderen Zwecken, z. B. im Bereich politischer Meinungsäußerungen, werden wohl nicht als Direktwerbung angesehen werden. Mit dem hier deutlich werdenden Problem der entsprechenden Grenzziehung wird sich der Bundesgesetzgeber bei der Umsetzung der Richtlinie zu befassen haben.

Die Position der Datenschutzbeauftragten sowohl auf nationaler als auch auf europäischer Ebene hierzu ist eindeutig: Sie werden für eine Stärkung des Einwilligungsmodells eintreten. Nur diese Lösung setzt nämlich das Grundrecht auf informationelle Selbstbestimmung konsequent um – erst fragen, dann handeln.

Der Auftrag der Kommission beim LfD, eine Orientierungshilfe für Newsletter-Dienste zu erarbeiten, wurde umgesetzt und die Handreichung den Abgeordneten zur Verfügung gestellt (vgl. Anlage 29).

Das Thema der unaufgeforderten Zusendung elektronischer Post mit politischem Inhalt war auch Gegenstand einer mittlerweile rechtskräftigen Entscheidung des Landgerichts München. Hier ging es zwar nicht um E-Mails von Abgeordneten, sondern um die unaufgeforderte Zusendung elektronischer Post einer politischen Partei an eine Anwaltskanzlei. Das Grundgesetz garantiert in Art. 21 den Parteien das Recht, bei der politischen Willensbildung des Volkes mitzuwirken. Im Ergebnis hat das Gericht festgestellt, dass eine Interessenabwägung ergibt, dass das Interesse des Empfängers an der Unterlassung der Beeinträchtigung seines Geschäftsablaufes überwiegt. Privatpersonen haben unter dem Aspekt des Eingriffs in das allgemeine Persönlichkeitsrecht einen entsprechenden Unterlassungsanspruch. Der politischen Partei sei deshalb zuzumuten, ihre Werbung auf die in ausreichender Zahl vorhandenen eingriffsärmeren Möglichkeiten wie etwa Plakate, Informationsstände sowie Verteilung von Flugblättern zu beschränken.

20.4 Novellierung des Rundfunkgebührenrechts

Die Datenschutzkonferenz hat am 30. April 2003 eine Entschließung verabschiedet, in der die zentralen datenschutzrechtlichen Kritikpunkte hinsichtlich der geplanten Neuordnung der Rundfunkfinanzierung genannt wurden (vgl. Anlage 23). Die darin geäußerten Befürchtungen bezogen sich auf den seinerzeit vorliegenden Entwurf zur Novellierung des Rundfunkgebührenstaatsvertrages. Dieser Verfahrensstand ist nicht mehr aktuell. Zwischenzeitlich gibt es einen Beschluss der Chefs der Staats- und Senatskanzleien der Länder, wonach der Gedanke der sog. Haushaltsgebühr nicht weiter verfolgt wird. Damit ist der Hauptkritikpunkt der genannten Entschließung aus dem Weg geräumt.

21. Technischer und organisatorischer Datenschutz

21.1 Kontroll- und Beratungstätigkeit

Im Berichtszeitraum sind in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung in 78 Fällen örtliche Feststellungen und Beratungen unter technisch-organisatorischen Gesichtspunkten erfolgt, u. a. bei folgenden Stellen:

- Aufsichts- und Dienstleistungsdirektion Trier
- Finanzministerium
- Fachhochschulen
- Schulen
- Krankenkassenrechenzentrum
- Kommunale Datenzentrale Mainz
- Krebsregister Rheinland-Pfalz
- Kreisverwaltungen
- Landesbetrieb Daten und Information Rheinland-Pfalz
- Landeshauptarchiv
- Landeskriminalamt
- Landesluftbild- und Rechenstelle
- Landesversicherungsanstalt
- Ministerien
- Oberfinanzdirektion
- Polizei- und Kriminalinspektionen
- Polizeipräsidien
- Rechenzentrum eines beauftragten Unternehmens
- Sparkassen
- Stadtverwaltungen
- Universitäten Mainz, Koblenz-Landau, Trier
- Universitätsklinikum Mainz
- Verbandsgemeinden
- Zentralstelle für Polizeitechnik.

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

Schwerpunkte der Prüfungs- und Beratungstätigkeit bildeten aufgrund aktueller Entwicklungen die Verfahren im Bereich der Polizei und des Einwohnermeldewesens.

Die Tendenz, den LfD bereits im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder im Zusammenhang mit der Erstellung von Sicherheitskonzepten zu beteiligen, hat sich weiter fortgesetzt. 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 Umwandlung des Daten- und Informationszentrums Rheinland-Pfalz in einen Landesbetrieb Daten und Information

Im Berichtszeitraum ist eine Neuorganisation und Änderung der Rechtsform des bisherigen Daten- und Informationszentrums (DIZ) erfolgt. Der LfD wurde bei der gutachterlichen Untersuchung im Vorfeld der Neuorganisation und im Rahmen des Gesetzgebungsverfahrens beteiligt. Die in seinem 17. Tb. (Tz. 14.6 und 14.7) dargestellten, für die datenschutzrechtliche Beurteilung solcher Vorhaben maßgebenden Gesichtspunkte sind in die Machbarkeitsstudie eingeflossen. Aus datenschutzrechtlicher Sicht entspricht die Fortführung des DIZ in Form eines Landesbetriebs der darin vertretenen Auffassung, wonach IT-Aufgaben mit wesentlicher Bedeutung im Rahmen hoheitlicher Tätigkeiten grundsätzlich durch öffentliche Stellen zu erbringen sind. Insbesondere gilt dies für die Bereiche Polizei, Justiz und Steuerverwaltung.

In seiner Stellungnahme hat der LfD weiterhin angeregt, klar zu stellen, dass mit der Umwandlung des DIZ in einen Landesbetrieb auch dessen datenschutzbezogene Aufgaben übergehen. Dem wurde entsprochen; dem künftigen Landesbetrieb obliegt nach § 1 Abs. 2 des LDI-Errichtungsgesetzes bei der Planung und dem Betrieb von IT-Verfahren im Rahmen seiner Unterstützungsaufgaben auch der technische Datenschutz. Eine entsprechende Aufgabenzuweisung wurde auch in die Betriebssatzung des LDI aufgenommen.

21.2.2 Landesdaten- und Kommunikationsnetz (rlp-Netz)

21.2.2.1 Sicherheitsanforderungen an die das rlp-Netz nutzenden Stellen

Dem Daten- und Informationszentrum oblag aus Sicht des LfD mit dem Betrieb des rlp-Netzes die Bereitstellung einer vertrauenswürdigen Infrastruktur. Für den Landesbetrieb Daten und Information als künftigem Betreiber des Landesnetzes gilt das Gleiche. Nach der gemeinsamen Auffassung des LfD und des LDI endet die Verantwortlichkeit des Landesbetriebs an den bei den Verwaltungen installierten rlp-Netz-Zugängen. Die Verantwortung für die Sicherheit der dahinter liegenden lokalen IT-Infrastruktur und deren Kommunikationsanbindungen zu Dritten (z. B. Fernwartungsanschlüsse) liegt hingegen bei den jeweiligen Verwaltungen.

In den als Rundschreiben veröffentlichten „Benutzungsbedingungen im landesweiten Datenübertragungsnetz“ aus dem Jahr 1994 (MinBl. 1994 S. 131) ist hierzu zwar eine entsprechende Abstimmung mit dem DIZ vorgesehen, die Erfahrung hat jedoch gezeigt, dass dem, wohl auch mangels Kenntnis der Regelung, vielfach nicht entsprochen wurde. Aufgrund der zunehmenden Integration der Netze hängt die Sicherheit des Landesnetzes jedoch in steigendem Umfang auch von der Sicherheit der IT-Strukturen der angeschlossenen Verwaltungen ab. Innerhalb des rlp-Netzes getroffene Sicherheitsmaßnahmen können durch dort vorhandene Defizite relativiert oder entwertet werden.

Der LfD hat daher angeregt, in den Verträgen mit den rlp-Netz-Teilnehmern verbindliche Sicherheitsanforderungen für einen Anschluss an das rlp-Netz vorzugeben. Weiterhin sollte, soweit sich aus Veränderungen lokaler IT-Strukturen Auswirkungen auf die Sicherheit des rlp-Netzes ergeben können, eine Pflicht zur Abstimmung mit dem LDI vertraglich vorgesehen werden.

21.2.2.2 Einsatz kryptografischer Verfahren im rlp-Netz

Der LfD hat im 18. Tb., Tz. 21.2.2.2 dargestellt, dass angesichts geänderter Rahmenbedingungen für das Landesnetz eine kryptografische Sicherung der Übertragungswege erforderlich ist. Aus fachlichen Überlegungen hatte auch die Polizei eine standardmäßige Leitungsverschlüsselung in dem von ihr genutzten Netzsegment gefordert. Entgegen der ursprünglichen Planung wird jedoch im rlp-Netz weiterhin nicht verschlüsselt.

Seitens des Ministeriums des Innern und für Sport und des LDI war zwar vorgesehen, entsprechende Lösungen im Subnetz der Polizei einzuführen, aufgrund nicht in der Verantwortung des LDI liegender technischer Probleme hat sich dies jedoch verzögert. Der Einsatz der Verschlüsselungsgeräte führte zu inakzeptablen Bandbreiteneinschränkungen, die auch durch den Hersteller der Geräte nicht behoben werden konnten. Hintergrund sind der hohe Vermaschungsgrad des rlp-Netzes und die Bandbreitenanforderungen insgesamt sowie für einzelne Fachverfahren. Das endgültige Ergebnis für die geplanten alternativen technischen Lösungen und die abschließende Entscheidung über das weitere Vorgehen stehen noch aus.

Dies ist hinsichtlich des Stellenwerts einer Verbindungsverschlüsselung für die Vertrauenswürdigkeit des rlp-Netzes unbefriedigend. Angesichts der wachsenden Bedeutung des rlp-Netzes als zentrale Kommunikationsplattform der Landesverwaltung wäre ein Verzicht auf die Verschlüsselung aus datenschutzrechtlicher Sicht bedenklich. Nicht zuletzt im Blick auf vergleichbare Bereiche, in denen sich eine Leitungsverschlüsselung als praktikabel erwiesen hat und standardmäßig genutzt wird (z. B. Kommunales Netz Rheinland-Pfalz, Informationsverbund Berlin-Bonn, TESTA-Netz) ist für das Landesnetz die Möglichkeit einer kryptografisch gesicherten Kommunikation erforderlich. Dies gilt insbesondere mit Blick auf das Auslaufen des bestehenden Netzvertrags und die für 2004 vorgesehene Neukonzeption des Landesnetzes.

Unabhängig davon ist bereits gegenwärtig eine Verschlüsselung auf ausgewählten Strecken technisch realisierbar. Dort, wo sensitive Informationen betroffen sind und die spezifischen Gegebenheiten des rlp-Netzes einer Verschlüsselung nicht entgegenstehen, sollte diese daher eingesetzt werden.

21.2.2.3 Internet- und Wählzugänge bei an das rlp-Netz angeschlossenen Verwaltungen

Der LfD wurde im Berichtszeitraum mehrfach um Stellungnahme zur Einrichtung von Internet-Anbindungen und Wählzugängen bei an das rlp-Netz angeschlossenen Verwaltungen gebeten. Hierzu hat er folgende Auffassung vertreten:

Bei der Einrichtung von Wählzugängen ist unter Sicherheitsaspekten zwischen verschiedenen Konstellationen zu differenzieren:

– Wählzugänge zum IT-System einer Verwaltung

  Zugriffsmöglichkeiten beschränken sich hierbei ausschließlich auf Daten und Anwendungen des IT-Systems der jeweiligen Verwaltung. In der Regel entspricht dies den Anforderungen bei der Anbindung von Außenstellen bzw. von Außendienstmitarbeitern der Verwaltung oder für Zwecke der Fernwartung. Mögliche Sicherheitsvorfälle können auf die innerhalb des lokalen Netzes erreichbaren Systeme beschränkt werden. Grundlegende Elemente einer datenschutzgerechten Lösung sind eine verlässliche Authentifizierung der Anschlusskomponenten und Teilnehmer, eine angemessene Sicherung personenbezogener Daten vor unbefugtem Zugriff und eine auf die dienstliche Notwendigkeit beschränkte Vergabe von Zugriffsrechten. Bei Berücksichtigung der genannten Voraussetzungen bestehen gegen die Einrichtung von Wählzugängen zu IT-Systemen der Verwaltungen aus datenschutzrechtlicher Sicht keine Bedenken. Die Verantwortung für deren sichere Einrichtung obliegt im Rahmen des Betriebs der lokalen IT-Lösungen der jeweiligen Verwaltung.

– Wählzugänge zu Anschlusskomponenten des rlp-Netzes

  Im Gegensatz zur vorgenannten Lösung eröffnet ein Zugang zum rlp-Netz grundsätzlich Kommunikationsmöglichkeiten mit allen angeschlossenen Verwaltungen und den Zugriff auf zentrale Systeme, Anwendungen und Dienste. Sicherheitsvorfälle sind damit in ihren Auswirkungen nicht auf IT-Einrichtungen einzelner Verwaltungen beschränkt, sondern können weite Teile des Landesnetzes betreffen. Der Verbindungsaufbau darf daher nur auf der Grundlage einer verlässlichen Identifikation und Authentifizierung der Teilnehmer erfolgen und muss eine Festverbindungen vergleichbare Sicherheit bieten. Hier bietet insbesondere der Einsatz kryptografischer Lösungen eine ausreichende Ende-zu-Ende-Sicherheit. Gleiches gilt für die Sicherung der Vertraulichkeit und Integrität der übertragenen Daten.

  Die Verantwortung für die Bereitstellung einer vertrauenswürdigen Kommunikationsinfrastruktur liegt beim Betreiber des rlp-Netzes, d. h. dem LDI. Sie erstreckt sich auf alle Netzkomponenten einschließlich der bei den Verwaltungen installierten Netzzugangspunkte. Soweit die Sicherheit des rlp-Netzes berührt ist, scheiden Lösungen, die nicht vom LDI mitgetragen werden, damit aus.

– Wählzugänge zum IT-System einer Verwaltung einschließlich der Möglichkeit eines Zugangs zum rlp-Netz

  Soweit Wählzugänge nicht zu separaten Zugangskomponenten des rlp-Netzes, sondern zu IT-Systemen von Verwaltungen eingerichtet werden, über diese jedoch ein Zugang zum rlp-Netz eröffnet wird, entspricht dies unter Sicherheitsaspekten der vorstehenden Konstellation. Damit sind auch in diesen Fällen die genannten Anforderungen zugrunde zu legen. Dies gilt auch für einen in Abstimmung mit dem LDI von einer Verwaltung für mehrere öffentliche Stellen betriebenen Wählzugang zum rlp-Netz (Einwahlknoten).

– Internet-Zugänge von Verwaltungen

  Zum gegenwärtigen Zeitpunkt verfügen nahezu alle Stellen der Landesverwaltung über einen Zugang zum rlp-Netz. Der Großteil nutzt über diesen auch den vom LDI betriebenen Internet-Zugang. Trotz dieser in vielen Fällen bestehenden Kopplung ist die Einrichtung einer Internet-Anbindung grundsätzlich unabhängig von einem rlp-Netz-Zugang. Die Firewall-Struktur am Internet-Übergang des rlp-Netzes deckt allerdings eine Reihe von Sicherheitsaspekten in angemessener Weise ab und bietet den Vorteil der Administration und des Betriebs nach einheitlichen Gesichtspunkten. Sie entbindet die angeschlossenen Verwaltungen auch davon, entsprechende technische und personelle Kapazitäten selbst vorzuhalten.

Eine datenschutzrechtliche Verpflichtung, Internet-Zugänge ausschließlich über den LDI als Betreiber des rlp-Netzes zu realisieren, besteht jedoch nicht. Die Realisierung eines Internet-Zugangs über Übertragungswege außerhalb des rlp-Netzes ist, ein vergleichbares Sicherheitsniveau vorausgesetzt, grundsätzlich möglich. So sind in einzelnen Verwaltungsbereichen Tendenzen erkennbar, den Weg ins Internet nicht über eine zentrale Gateway-Lösung, sondern über Einzelanbindungen zu realisieren. Eine datenschutzgerechte Internet-Anbindung erfordert, dass den daraus resultierenden Gefährdungen angemessen Rechnung getragen wird. Angesichts der bestehenden Risiken ist diese nur vertretbar, wenn zuvor in einem Sicherheitskonzept eine Analyse und Bewertung der Risiken erfolgt ist und den Gefahren durch technische und organisatorische Maßnahmen hinreichend begegnet wird (vgl. 17. Tb., Tz. 21.3.5). Dies bleibt nach den Erkenntnissen des LfD bei den Überlegungen häufig unberücksichtigt. Vielfach werden der Entscheidung lediglich die reinen Kommunikationskosten zugrunde gelegt und Aufwendungen für notwendige Sicherheitsmaßnahmen nicht mit einbezogen.

21.2.3 Europäisches Kommunikationsnetz der Verwaltungen (TESTA-Netz)

Zweck und Konzeption des TESTA-Netzes, eines Netzzusammenschlusses für die länderübergreifende Verwaltungskommunikation, wurden im 17. Tb. (Tz. 21.2.8) dargestellt. Der LfD hatte in Übereinstimmung mit den Datenschutzbeauftragten aller angeschlossenen Länder auf die Notwendigkeit der Leitungsverschlüsselung innerhalb des TESTA-Netzes hingewiesen.

Dem wurde zwischenzeitlich entsprochen. Die Kommunikation zwischen den Netz-Zugangspunkten der einzelnen Länder wird über kryptografische Verfahren abgesichert und gewährleistet eine angemessene Vertraulichkeit, die Integrität der Daten sowie Authentizität der Kommunikationsteilnehmer. Die Verschlüsselung endet gegenwärtig am Übergang des TESTA-Netzes zum rlp-Netz (vgl. Tz. 21.2.2.2). Für eine gegebenenfalls erforderliche durchgängige Absicherung der Kommunikation vom Absender bis zum Empfänger sind damit ergänzende Maßnahmen auf Anwendungsebene erforderlich.

Bei den an das TESTA-Netz angeschlossenen Stellen handelt es sich um einen festgelegten Teilnehmerkreis, der bestimmten Anschlussvoraussetzungen unterliegt. Im Vergleich zu öffentlichen Netzen ergeben sich damit geringere Sicherheitsrisiken. Gleichwohl bedarf es im Rahmen der Anbindung des Landesnetzes Vorkehrungen, die sicherstellen, dass Protokolle und Dienste nur im zugelassenen Umfang genutzt werden können. Den diesbezüglichen Empfehlungen des LfD hat der LDI mit seiner Firewallstruktur für die Absicherung des Übergangs des rlp-Netzes zum TESTA-Netz entsprochen.

21.2.4 Kommunales Netz Rheinland-Pfalz (KNRP)

21.2.4.1 Struktur und Sicherheitsaspekte des Kommunalen Netzes Rheinland-Pfalz

Mit der Inbetriebnahme des Verfahrens EWOIS-neu (vgl. Tz. 21.2.5) ging für den Großteil der kommunalen Verwaltungen ein Wechsel der Kommunikationsplattform einher. Für die Städte und Gemeinden wurde das „Kommunale Netz Rheinland-Pfalz“ (KNRP) gebildet, dessen wesentliches Sicherheitsmerkmal die hardwareseitige Verschlüsselung der Kommunikationswege ist. Angesichts der Bedeutung , die dem KNRP als künftige zentrale Plattform der elektronischen Kommunikation zukommen wird, ist die standardmäßige Leitungsverschlüsselung ausdrücklich zu begrüßen. Ursprünglich als völlig eigenständiges Netz geplant ist die Realisierung des KNRP nunmehr auf Grundlage des rlp-Netzes erfolgt, in welchem das KNRP als logisches Teilnetz betrieben wird. Hierdurch ergeben sich besondere Beziehungen der beteiligten Stellen zueinander: Betreiber des KNRP ist im Auftrag der Komm-Wis ein Konsortium aus T-Systems und der KDZ-Mainz. Unterauftragnehmer des Konsortiums für den technischen Betrieb des KNRP und die Administration der Netzkomponenten ist der LDI, der gleichzeitig (vgl. Tz. 21.2.5.6) im Rahmen des EWOIS-neu-Betriebs eine Aufsichtsfunktion hat. In deren Rahmen werden vom LDI zentrale administrative Aufgaben wahrgenommen. Hierzu zählen insbesondere die Verwaltung der Verschlüsselungskomponenten des so genannten Netzsegments „VPN-E“, in welchem die Kommunikation des EWOIS-neu-Verfahrens abgewickelt wird.

21.2.4.2 Anbindung von Kommunen im KNRP an zentrale Verfahren des LDI

Da das KNRP künftig als eigenständiges logisches Teilnetz innerhalb des rlp-Netzes betrieben wird, ergibt sich die Notwendigkeit einer kontrollierten Kommunikation zu anderen Teilnetzen des Landesnetzes. Im Rahmen seiner Aufsichtsfunktion soll hier vom LDI ein gesicherter Übergang vom KNRP zum rlp-Netz erfolgen, so dass kommunale Verwaltungen auf zentrale Verfahren des LDI zugreifen können. Dieser Punkt ist besonders bedeutsam, da nach dem bisherigen Sicherheitskonzept zwischen logischen Teilnetzen des rlp-Netzes keine Übergänge bestanden. Die Empfehlungen des LfD hinsichtlich einer Filterung nach Quell- und Zieladresse sowie den verwendeten Protokollen und Diensten wurden aufgegriffen.

21.2.4.3 Bildung von Kreisdatennetzen

Neben der Nutzung zentraler Verfahren im LDI werden von kommunalen Verwaltungen auch eigene Verfahren betrieben, die über Datennetze von anderen Verwaltungen genutzt werden. Insbesondere im Bereich der Kreisverwaltungen wurden so genannte Kreisdatennetze gebildet, in denen die kreisangehörigen Gemeindeverwaltungen mit den jeweiligen Kreisverwaltungen kommunizieren. Entsprechend den Empfehlungen des LfD basieren die logischen Verbindungen zwischen den teilnehmenden Verwaltungen auf statischen Routen, die aufgrund eindeutiger Erklärungen der teilnehmenden Verwaltungen durch den Netzbetreiber

geschaltet wurden. Sollten die Kreisverwaltungen künftig im rlp-Subnetz „Verwaltung“ verbleiben, würde diese Form der Kommunikation entsprechend den Empfehlungen des LfD im Rahmen der Aufsichtsfunktion des LDI durch entsprechende Filterung am Netzübergang zusätzlich abgesichert.

Im Rahmen des Betriebs von EWOIS-neu wird derzeit an zwei Stellen im Land ein besonderer Zugang zum KNRP praktiziert. Die hierbei beteiligten Verwaltungen stellen über eigene VPN-Lösungen Verbindungen zu zentralen Knoten her, die ihrerseits dann den KNRP-Anschluss realisieren. In beiden Fällen erfolgt die Verbindung über kryptografisch gesicherte Tunnelverbindungen zu den zentralen Knoten. Die definierten Verbindungsregeln entsprechen den Empfehlungen des LfD.

21.2.5 Einwohnerinformationssystem Rheinland-Pfalz (EWOIS)

21.2.5.1 EWOIS-Komponente MESO

Was lange währt – wird doch noch gut! Unter diesen Leitsatz könnte man auch die Neuentwicklung des Einwohnerinformationssystems MESO stellen. Zum 1. April 2003 wurde in den Kommunen durch die Firma KommWis GmbH das neue „dezentrale“ (siehe hierzu auch Tz. 21.2.5.4) Einwohnerinformationssystem in Betrieb genommen. Das seit 1971 betriebene Großrechnerverfahren EWOIS gehört damit der Vergangenheit an.

Mit der Einführung von MESO steht den Kommunen ein Verfahren zur Verfügung, das sie grundsätzlich selbst betreiben können. Ihren Forderungen entsprechend sind sie damit in die Lage versetzt worden, Einwohnerdaten ohne Einschaltung eines Dritten und somit ohne zusätzliche Kostenanforderungen (z. B. für einzelne Listen) selbst zu verarbeiten.

Mit der Neuentwicklung wurde auch die Möglichkeit geschaffen, formal das Verfahren so zu gestalten, dass den Datenschutzanforderungen des Meldegesetzes stärker entsprochen werden kann. Beispielsweise

– können nunmehr alle nach dem Meldegesetz möglichen Auskunftssperren im Meldedatensatz gespeichert werden,

– ist es möglich, die Zugriffsrechte so zu vergeben, dass nur die für die jeweilige Sachbearbeitung erforderlichen Informationen zur Verfügung gestellt werden können,

– ist eine Protokollierung realisiert, die es ermöglicht nachzuvollziehen, wer wann auf welche Daten zugegriffen hat.

Den früheren Forderungen des LfD (zuletzt siehe 17. Tb. Tz. 4) wurde somit in weiten Teilen Rechnung getragen.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass die Kommunen nunmehr grundsätzlich selbst in der Lage sind zu entscheiden, wer gemäß § 31 Abs. 7 MG innerhalb ihrer Verwaltung auf welche Meldedaten Zugriff haben soll. Nach wie vor sind vor der Einrichtung einer Zugriffsmöglichkeit die Voraussetzungen des § 7 LDSG zu prüfen. Das Ergebnis der Überprüfung ist schriftlich zu dokumentieren. Zur Erleichterung hat das Ministerium des Innern und für Sport hierzu in Abstimmung mit dem LfD Musterdienstanweisungen über den automatisierten Abruf von Meldedaten innerhalb der Gemeinde-/Verbandsgemeinde-/Stadtverwaltung erarbeitet.

Leider ist es jedoch auch mit dem neuen Verfahren MESO bisher nicht möglich, der in § 11 MG detailliert geregelten Löschung und Aufbewahrung von Meldedaten gerecht zu werden. Die im bisherigen Verfahren enthaltenen Archivdaten wurden auch in MESO übernommen. Eine Löschung bzw. Archivierung ist nicht erfolgt. Gründe hierfür waren neben der bei der Einführung noch fehlenden Funktionalität die Abhängigkeiten der einzelnen Informationen untereinander.

Der LfD hat in der Vergangenheit mehrfach diesen Missstand problematisiert und darauf hingewiesen, dass es zwingend notwendig sei, Meldedaten entsprechend § 11 MG zu archivieren bzw. zu löschen. Um dem nachzukommen, entwickelt derzeit die Fa. KommWis GmbH gemeinsam mit dem Hersteller von MESO ein entsprechendes Modul.

Die durchgeführten örtlichen Feststellungen im Bereich MESO haben neben einigen allgemeinen datenschutzrechtlichen Hinweisen bisher zu keinen Beanstandungen geführt. Der LfD wird auch weiterhin den datenschutzgerechten Einsatz dieses Verfahrens bei den Kommunen kontrollieren.

21.2.5.2 EWOIS-Komponente Integrationssystem

Im Integrationssystem sind Teile der einzelnen dezentralen Datenbestände des Verfahrens MESO zentral zusammengefasst. Dieser zentrale Datenbestand dient zunächst der Übernahme der Daten eines Einwohners bei Zuzug bzw. Wegzug. Darüber hinaus werden aus dem zentralen Datenbestand auch zentrale Verfahrensfunktionen wahrgenommen. Hierbei handelt es sich derzeit noch ausschließlich um die regelmäßigen Datenübermittlungen an bestimmte Empfänger (wie z. B. Kirchen, Rentenstellen, Bundeswehr im Rahmen der Wehrerfassung). Fallweise können auch Datenabgleiche des zentralen Meldedatenbestands mit vom Auftraggeber zur Verfügung gestellten Dateien durchgeführt werden. Der LfD hat die Entwicklung des Integrationssystems von Anfang an begleitet und im Pilotbetrieb kontrolliert. Grundsätzliche datenschutzrechtliche Bedenken haben sich dabei nicht ergeben. Der LfD wird die Ausgestaltung und Nutzung des Integrationssystems im Rahmen örtlicher Feststellungen im Zusammenhang mit dem Gesamtkomplex des neuen Einwohnerinformationssystems weiter kontrollieren.

21.2.5.3 EWOIS-Komponente Informationssystem

Für die Abfrage von Meldedaten durch Stellen der Landesverwaltung steht im Verfahren EWOIS-neu die Komponente Informationssystem zur Verfügung. Das Informationssystem enthält im Vergleich zu den lokalen Datenbeständen der Meldebehörden (Tz. 21.2.5.1) und dem Integrationssystem (Tz. 21.2.5.2) nur einen Teil des Gesamtbestands (Informationssystem ca. 30 Datenbanktabellen, Integrationssystem ca. 70 Tabellen, dezentraler MESO-Bestand ca. 200 Tabellen). Es dient vorrangig als Auskunftssystem für aktuelle Fälle im Wege der Einzel- bzw. Gruppenauskunft. Die im bisherigen Verfahren erfolgten Datenabgleiche und Datenübermittlungen werden künftig ausschließlich auf der Basis des Integrationssystems durchgeführt.

Hinsichtlich der notwendigen Mechanismen zur Steuerung des Zugriffs entspricht das Informationssystem den im 18. Tb., Tz. 21.2.1.1 dargestellten Empfehlungen des LfD. Auf der Grundlage eines X.500-Verzeichnisdienstes ist eine Steuerung von Zugriffen und Auswertungen nach Art der Verwaltungen, Benutzergruppen/Benutzern, regionaler Zuständigkeit und fachlichen Anforderungen möglich. Die Definition der funktionalen Behörden (Rollen) und deren Zugriffsrechte im Informationssystem erfolgt dabei zentral. Die abfragenden Stellen haben die Möglichkeit, innerhalb der ihnen zugewiesenen Rollen selbständig Benutzer einzurichten und zu pflegen. Die vorhandenen Protokollierungsmechanismen erlauben es, den Umfang zu protokollierender Zugriffe bezogen auf die abfragende Stelle und die Art des Zugriffs (Einzel- oder Gruppenauskunft) variabel vorzugeben.

Eine Sondersituation ergibt sich für den Bereich der Polizei. Die Prüfung der EWOIS-Berechtigung stützt sich dabei, abweichend gegenüber dem Zugang sonstiger Stellen, auf einen eigenen Verzeichnisdienst der Polizei. Angesichts des einheitlichen Rechteprofils der polizeilichen Nutzer und des reduzierten Aufwands für die Datenpflege bestanden hiergegen keine Bedenken. Kern der Empfehlungen des LfD war in diesem Zusammenhang, dass gewährleistet sein muss, erfolgte Datenzugriffe bei Bedarf konkreten Personen zuordnen zu können; dem wurde entsprochen.

Für die Kommunikation der abrufenden Stelle mit dem Informationssystem kommt eine SSL-Verschlüsselung zum Einsatz, so dass auch im Blick auf die gegenwärtig noch ausstehende Leitungsverschlüsselung im rlp-Netz (vgl. Tz. 21.2.2.2) eine ausreichende Vertraulichkeit der Abrufe gewährleistet ist.

Im Rahmen der Datenmigration aus dem Vorläuferverfahren wurden aus technischen Gründen Angaben früherer Wohnsitze übernommen, die über den in der Verfahrenskonzeption vorgesehenen Zeitraum hinausgehen. Im Blick auf die o. g. Auskunftsfunktion des Informationssystems lediglich für aktuelle Meldedaten hat der LfD dies problematisiert. Eine Bereinigung des Datenbestandes ist mit der Einführung einer Archivierungskomponente in MESO vorgesehen, die die Speicherung dieser Angaben im Informationssystem entbehrlich macht (vgl. Tz. 21.2.5.1).

21.2.5.4 Hosting-Betrieb der dezentralen Meldedatenbanken

Im Laufe der Entwicklung des neuen Einwohnerinformationssystems hat sich bei zahlreichen Kommunen die Erkenntnis eingestellt, dass mit der Dezentralisierung des Einwohnerinformationssystems ein enormer Aufwand entsteht und für die Betreuung hoher technischer Sachverstand erforderlich ist.
Dies hat die Kommunale Datenzentrale Mainz (KDZ) zum Anlass genommen, das sog. Hosting-Modell den Kommunen anzubieten. Aufgabe des Systems ist die Zentralisierung der Datenhaltung und der damit verbundenen Administration. Zur Realisierung des Modells betreibt die KDZ hierzu eine „Serverfarm“.

Ursprünglich war in Erwägung gezogen worden, entsprechend dem konsolidierten Gesamtbestand der MESO-Daten – dem Integrationssystem – die einzelnen Datenbestände in einer gemeinsamen Datenbank abzulegen. Der LfD hat hiergegen datenschutzrechtliche Bedenken geäußert, nicht zuletzt wegen der Möglichkeit, dass die Meldedaten auch bestandsübergreifend ausgewertet werden könnten. Die KDZ hat diesen Bedenken Rechnung getragen und betreibt nunmehr für jede einzelne Kommune eine separate „Oracle-Instanz“, auf der die Meldedatenbestände abgelegt sind. Bestandsübergreifende Auswertungen sind damit nicht mehr möglich.

Zwischenzeitlich haben sich von 212 Kommunen 170 für eine Teilnahme an diesem System entschieden.

Auch aus datenschutzrechtlicher Sicht ist diese Entwicklung – zurück von der Dezentralisierung – nicht ohne Vorteil. So ist es nicht mehr zwingend erforderlich, zentrale datenschutzrechtliche Forderungen gegenüber jeder einzelnen Kommune geltend zu machen. Vielmehr besteht die Möglichkeit, auftretende Probleme an zentraler Stelle mit der KommWis GmbH und der KDZ zu erörtern, wodurch ein einheitlicher Datenschutzstandard realisierbar ist.

Im Rahmen örtlicher Feststellungen zum Hosting-Modell hat der LfD in der Vergangenheit einige datenschutzrechtliche Hinweise gegeben, deren Umsetzung er im Rahmen künftiger örtlicher Feststellungen kontrollieren wird.

21.2.5.5 Privatisierung des Betriebs des Einwohnerinformationssystems EWOIS-neu

Der Betrieb zentraler Komponenten des Einwohnerinformationssystems wurde im Rahmen einer Ausschreibung an ein Konsortium bestehend aus der T-Systems GmbH – einer Tochtergesellschaft der Deutschen Telekom – und der Kommunalen Datenzentrale Mainz vergeben. Die Betriebsaufgaben gehen dabei über den rein technischen Betrieb der Systeme und die Datenhaltung hinaus und umfassen auch die Wahrnehmung zentraler Verfahrensfunktionen.

Vor dem Hintergrund, dass die Betriebsübernahme durch eine nichtöffentliche Stelle mit einem Wegfall der im Rahmen der Rechts- und Fachaufsicht bestehenden direkten Einwirkungsmöglichkeiten verbunden ist, hat der LfD die Notwendigkeit betont, dies durch eine entsprechende Vertragsgestaltung und geeignete technisch-organisatorische Maßnahmen zu kompensieren. Insbesondere gelte dies für die Bereiche Transparenz des Verfahrensablaufs und Dokumentationspflichten, Nachvollziehbarkeit der Verarbeitung, Weisungsrechte, Informationspflichten, Steuerungs- und Kontrollmöglichkeiten, Rückholbarkeit und Sanktionsmöglichkeiten bei Verstößen. Entsprechende Vorgaben wurden in den Betriebsverträgen für das Intergrations- und Informationssystem sowie das Kommunale Netz berücksichtigt.

In verschiedenen Bereichen des Verfahrens wurden durch den LfD örtliche Feststellungen getroffen. Ziel war es dabei zu klären, inwieweit das Betriebskonzept und die Betriebspraxis den genannten Vorgaben entsprechen. Die Erkenntnisse zeigen, dass Outsourcing-Lösungen bei komplexen Großverfahren wie EWOIS-neu datenschutzrechtlich einer differenzierten Betrachtung bedürfen.

So basiert der Verfahrensbetrieb durch T-Systems auf professionellen personellen, organisatorischen und technischen Strukturen. Insbesondere der Rechenzentrumsbetrieb und die für die Betreuung der Systeme genutzten Kommunikationsnetze genügen den notwendigen Sicherheitsanforderungen; vielfach gehen sie darüber hinaus.

Gleichwohl schränkt eine Auslagerung die Möglichkeiten der Auftraggeber, die Organisation des Verfahrensbetriebs zu bestimmen, letztlich ein; jedenfalls erschwert sie die Beurteilung, welche Daten für welche Stellen im Zugriff stehen. Die Entscheidung über die Betriebsstandorte entzieht sich teilweise dem Einfluss der Auftraggeber. So sind am Betrieb des EWOIS-Verfahrens Betriebseinheiten in mehreren Bundesländern beteiligt, wobei gegenüber den Auftraggebern zunächst offen bleibt, welche Stellen konkret mit welchen Aufgaben betraut sind und in welcher Vertragsbeziehung diese zum Auftragnehmer stehen. Hintergrund solcher Informationsdefizite sind vorrangig Veränderungen von Unternehmensorganisationen, ausgelöst beispielsweise von Marktentwicklungen, Verbesserungen der Kostenstruktur, Optimierung betrieblicher Abläufe und Unternehmensbeteiligungen. Grundsätzlich bestünde zwar die Möglichkeit, eine bestimmte Betriebsorganisation vertraglich festzuschreiben, die damit verbundenen finanziellen Auswirkungen wirken jedoch der mit einer Auslagerung angestrebten Kostenreduzierung entgegen. Aus datenschutzrechtlicher Sicht bedarf es damit verlässlicher Vereinbarungen über Informationspflichten im Fall von Änderungen des Verfahrensbetriebs.

Für das Verfahren EWOIS-neu hat sich auch die Forderung des LfD als bedeutsam erwiesen, die Betriebsstandorte auf das Gebiet der Bundesrepublik Deutschland zu beschränken. Das genutzte Rechenzentrum ist Teil einer globalen Struktur, so dass grundsätzlich auch IT-Strukturen außerhalb Deutschlands oder Europas nutzbar wären. Die Frage, ob und wie Kontrollrechte der Auftraggeber oder des Datenschutzbeauftragten in solchen Fällen wirksam ausgeübt werden können, kann angesichts der bestehenden Lösung dahinstehen.

Unverzichtbar für die Ausübung von Weisungs- und Kontrollrechten des Auftraggebers sowie für die vorbehaltene Rückholbarkeit des Verfahrens ist eine ordnungsgemäße Dokumentation im Sinne des § 9 Abs. 2 Nr. 9 LDSG. Solange dies nicht der Fall ist, muss eine vertraglich vorgesehene Möglichkeit der Kündigung und Übernahme des Verfahrens durch einen Dritten relativiert werden. Im Bereich der Dokumentation bestehen aus Sicht des LfD noch Defizite des Verfahrens. So liegen zugesagte und für den Betrieb des Verfahrens wesentliche Dokumentationen und Nachweise bislang nicht vor.

Datenschutzrechtlich von Bedeutung ist weiterhin die Möglichkeit strafrechtlicher Sanktionen im Missbrauchsfall. Wesentlich ist hierbei eine formelle Verpflichtung nach dem Verpflichtungsgesetz der mit wesentlichen operativen Betriebsaufgaben betrauten Personen. Bei hochdiversifiziertem Betriebsablauf wie im Fall von EWOIS-neu kann dies mit betrieblichen Belangen des Auftragnehmers kollidieren. Die Klärung der diesbezüglichen Fragen hat sich als zeitaufwändig erwiesen, wodurch die zugesagte Verpflichtung des o. g. Personenkreises zum Zeitpunkt der Vorlage dieses Berichts noch nicht abgeschlossen war.

Die genannten Probleme sind zum Teil auf die mit der Übernahme eines Großverfahrens verbundenen Anlaufschwierigkeiten zurückzuführen. Trotz offener Fragen haben sich bislang allerdings keine Feststellungen ergeben, aufgrund derer die Auslagerung des EWOIS-Betriebs datenschutzrechtlich zu beanstanden wäre. Neben der Klärung der angesprochenen offenen Punkte sind im weiteren Verlauf ergänzende Kontrollen des Verfahrens vorgesehen.

21.2.5.6 Aufsichtsfunktion des LDI beim Betrieb des Verfahrens EWOIS-neu

Der technische Betrieb des Verfahrens EWOIS-neu liegt wie unter Tz. 21.2.5.5 dargestellt zum großen Teil in der Hand eines privaten Unternehmens als Auftragnehmer. Die enge Verzahnung des Verfahrens EWOIS-neu mit dem Kommunalen Netz sowie dem rlp-Netz hätte es nach den ursprünglichen Vorstellungen erfordert, den Auftragnehmer als Teilnehmer in das rlp-Netz einzubinden. Hiergegen wurden im Blick auf dessen nichtöffentlichen Charakter seitens des LfD Bedenken geäußert. Er hat empfohlen, die betroffene Steuerung und Kontrolle der Verbindungswege in der Hand einer der Landesaufsicht unterstehenden Stelle zu belassen.

Dem wurde dadurch entsprochen, dass diese Aufgabe durch den LDI für den Betreiber des Kommunalen Netzes wahrgenommen wird. Die notwendige technische Infrastruktur befindet sich zurzeit im Aufbau. Die Aufsichtsfunktion umfasst dabei im Wesentlichen drei Bereiche:

– die Administration der Kommunikationswege für Verbindungen zwischen dem rlp-Netz und dem Kommunalen Netz (KNRP),
– den Betrieb einer Firewall am Übergang des Kommunalen Netzes zum Rechenzentrum des Verfahrensbetreibers und
– die Administration der Netzkomponenten bei den Teilnehmern des Kommunalnetzes.

Die vom LfD geforderte Unabhängigkeit des LDI bei der Wahrnehmung der Aufsichtsfunktion wird mit einer vertraglichen Vereinbarung gewährleistet, nach der dem Betreiber des Kommunalnetzes bzw. des Verfahrens EWOIS-neu in diesem Bereich grundsätzlich kein Weisungsrecht zukommt. Änderungen des zugrunde liegenden Sicherheitskonzeptes sind nur einvernehmlich nach einem geordneten Verfahren möglich.

21.2.6 ISDN-Nebenstellenanlage der Landesregierung

Für die Abwicklung des Telefon- und Faxverkehrs sowie verschiedener elektronischer Kommunikationsdienste wird für den Bereich der Landesregierung eine gemeinsam genutzte digitale Telefonanlage mit insgesamt ca. 3 500 Nebenstellen eingesetzt. Im Rahmen örtlicher Feststellungen wurde die Anlagenkonfiguration überprüft.

Hinsichtlich der Konfiguration von Leistungsmerkmalen, die ein Mithören von Gesprächen erlauben, haben sich dabei keine Auffälligkeiten ergeben. Sie entsprach den Vorgaben der getroffenen Dienstvereinbarung, insbesondere ist eine akustische bzw. optische Signalisierung gewährleistet, die ein etwaiges Mithören erkennbar macht. Zur Speicherung von Gesprächsdaten hat der LfD Empfehlungen ausgesprochen, denen noch im Rahmen der Kontrolle entsprochen wurde.

Von den vorhandenen Datenanschlüssen ergab sich für ca. 70 Nebenstellen Klärungsbedarf. Diese waren ausdrücklich als Modem- oder vergleichbare Datenkommunikationsanschlüsse ausgewiesen, wobei die vorliegenden Informationen keine Einordnung des zugrunde liegenden Zwecks erlaubten. Die Angaben lieferten fallweise Hinweise darauf, dass der jeweilige Anschluss als Zugang zu lokalen IT-Systemen diente bzw. als Internet-Anbindung genutzt wurde.

Eine Internet-Anbindung der Ressorts erfolgt in der Regel über den Anschluss der Ministerien an den zentralen Internet-Übergang des Landesdaten- und Kommunikationsnetzes. Den aus einer Internet-Anbindung resultierenden Gefährdungen wird dabei mit der Firewall-Struktur des LDI begegnet. Zugänge, die nicht über die gesicherte Anbindung erfolgen, wie separate Modemverbindungen am Arbeitsplatz, stellen das damit gewährleistete Sicherheitsniveau des Landesnetzes in Frage und bergen im Fall vernetzter Systeme das Risiko unbefugter Übergriffe in die IT-Netze der jeweiligen Verwaltungen. Derartige „Hintertüren“ ins Internet sind daher nach den Empfehlungen des LfD grundsätzlich zu untersagen und soweit möglich technisch zu unterbinden (17. Tb., Anlage 22, Tz. 2.).

Eine Reihe weiterer Nebenstellen verfügte über die technische Ausstattung, die den Nutzern eine selbständige Einrichtung als Datenkommunikationsanschluss ermöglichte. Hintergrund waren ursprüngliche Überlegungen zu einer Rechnervernetzung über die TK-Anlage, die nach dem Aufbau des Lichtwellenleiternetzes der Ministerien jedoch nicht weiter verfolgt wurden.
Auf Empfehlung des LfD hin wurde die Konfiguration der betroffenen TK-Anschlüsse überprüft und erforderlichenfalls angepasst.

21.2.7 IT-Anbindung von Ministerien bei einem Dienstgebäudewechsel

Im Rahmen eines vorübergehenden Umzugs von Ministerien war die Nutzung von Kommunikationsstrecken der Universität Mainz vorgesehen. Betroffen war die gesamte elektronische dienstliche Kommunikation, d. h. neben der Sprachkommunikation die E-Mail-Kommunikation im Ressortbereich, mit anderen Stellen der Landesregierung, der Landesverwaltung und des Bundes.

In seiner Stellungnahme hat der LfD auf die im Fall einer Anbindung der Ministerien über die Leitungswege der Universität zugrunde zu legenden Anforderungen an eine vertrauenswürdige Kommunikation hingewiesen (vgl. 18. Tb., Tz. 21.2.2.2). Angesichts der bestehenden Rahmenbedingungen im universitären Bereich und der Nutzung des offenen IP-Protokolls bestand aus Sicht des LfD die Notwendigkeit, die Übertragungswege durch kryptografische Verfahren abzusichern. In gleicher Weise wurde in der Vergangenheit bereits bei der Nutzung von Kommunikationsverbindungen im Hochschulbereich für das rlp-Netz verfahren.

Aufgrund der Vielfalt der Kommunikationsvorgänge sollte dabei einer Leitungsverschlüsselung über die Bildung eines Virtuellen Privaten Netzes (VPN) der Vorzug vor anwendungsorientierten Lösungen gegeben werden. Die z. B. im Bereich des Kommunalen Netzes Rheinland-Pfalz eingesetzte Lösung stellt geeignete Mechanismen bereit und begegnet keinen datenschutzrechtlichen Bedenken.

Im Blick auf die für die Sprachkommunikation nur mit unverhältnismäßigem Aufwand mögliche Verschlüsselung hat der LfD von einer konkreten Empfehlung zur kryptografischen Absicherung der Telefonie und des Telefaxverkehrs abgesehen, soweit dies nicht über das IP-Protokoll erfolgt. Er hat jedoch die Notwendigkeit betont, in vertraglicher Hinsicht die Universität den gleichen Verschwiegenheitsanforderungen zu unterwerfen wie den ansonsten von der Landesverwaltung in Anspruch genommenen Provider.

21.2.8 Jugendgemeinderatswahl via Internet

Im Rahmen einer Jugendgemeinderatswahl wurde in einer Gemeinde die Möglichkeit der Stimmabgabe per Internet eröffnet. Zur Wahrung des Wahlgeheimnisses wurde eine anonyme Verfahrensweise mit Transaktionsnummern (TAN) gewählt. Bei dieser war die Zuordnung der TAN zu einer bestimmten Person nur der Gemeindeverwaltung möglich, die Zuordnung der TAN zur konkreten Stimmabgabe nur der mit der technischen Durchführung beauftragten Firma.

Seitens des LfD wurde u. a. problematisiert, dass für die Gemeindeverwaltung weitgehend keine Steuerungs- oder Einwirkungsmöglichkeiten auf die technische Durchführung der Wahl bestanden. Weiterhin war ein Prüfungs- und Freigabeverfahren für die eingesetzte Software nicht vorhanden, so dass die Ordnungsmäßigkeit des Programmablaufs bei Stimmenabgabe und -verteilung nicht anhand eindeutiger Kriterien, z. B. Prüfsummen, belegt werden konnte (vgl. 15. Tb., Tz. 21.2.2). Weitere Anmerkungen des LfD betrafen die Dokumentation des Verfahrens.

Die Feststellungen des LfD haben ergeben, dass bei der Vorbereitung der Wahl weniger wahlrechtliche Aspekte im Vordergrund standen, als vielmehr das Bemühen, mit der Wahlmöglichkeit via Internet die Attraktivität des Wahlgangs für die betroffene Gruppe von Wahlberechtigten zu steigern (die Wahlbeteiligung lag im vorliegenden Fall bei ca. 5 %; etwa $^3/_5$ der Stimmen wurden per Internet abgegeben).

Im Blick auf die vergleichsweise überschaubare Bedeutung der Wahl wurden die Vorkehrungen zur Wahrung des Wahlgeheimnisses letztlich als ausreichend angesehen. Für den Fall, dass entsprechende Verfahren z. B. im Rahmen von Kommunalwahlen eingesetzt werden sollten, ergeben sich allerdings klärungsbedürftige Punkte.

21.2.9 Optische Archivierung im Bereich Führerscheinwesen

Im Rahmen der Neugestaltung eines entsprechenden Verfahrens wurde der LfD um eine Stellungnahme zur optischen Archivierung gebeten.

In technischer Hinsicht sind dabei insbesondere die datenschutzrechtlichen Anforderungen an die Berichtigung, Sperrung und Löschung gespeicherter Daten (§ 19 LDSG) sowie die Sicherstellung der Integrität von Bedeutung. So ist bei der Speicherung oder Archivierung von Daten auf nur einmal beschreibbaren optischen Datenträgern durch eine geeignete Organisation sicherzustellen, dass Löschungsvorgaben eingehalten werden können. Unter den Voraussetzungen des § 19 Abs. 3 LDSG kann an die Stelle einer Löschung die Sperrung treten. Die solcherart gesperrten Daten sind besonders zu kennzeichnen. Spätestens nach dem vollständigen Beschreiben des Datenträgers ist nach dem vorstehenden Verfahren die endgültige Löschung vorzusehen.

Für die Integritätssicherung elektronisch archivierter Dokumente, an die besondere Anforderungen hinsichtlich ihrer Vollständigkeit, Korrektheit oder des Nachweises der Urheberschaft gestellt werden, sollte auf elektronische Signaturverfahren zurückgegriffen werden. Das in dieser Hinsicht mit einer qualifizierten Signatur nach § 2 Nr. 3 SigG verbundene Schutzniveau ist nur dort von Bedeutung, wo entsprechende gesetzliche Vorgaben oder besondere Anforderungen an Authentizität und Integrität elektronischer Daten bestehen. Bei geeigneten technisch-organisatorischen Rahmenbedingungen kommen damit grundsätzlich auch fortgeschrittene Signaturlösungen nach § 2 Nr. 2 SigG in Betracht.

21.2.10 Verschlüsselung von Identitätsdaten im Krebsregister Rheinland-Pfalz

Die Identitätsdaten der im Krebsregister Rheinland-Pfalz eingestellten Datensätze sind nach § 8 Abs. 1 LKRG zu verschlüsseln. Die hierfür bislang eingesetzte Lösung ging auf ein Verfahren zurück, das für die Erprobungsphase des Registers entwickelt wurde. Der LfD hatte in diesem Zusammenhang den Umstieg auf ein vom Bundesamt für Sicherheit in der Informationstechnik entwickeltes Verfahren empfohlen. Dem wurde zwischenzeitlich entsprochen.

Der dabei notwendige Schlüsselwechsel erfordert die Entschlüsselung und anschließende Neuverschlüsselung der Identitätsdaten des gesamten Registerbestandes (§ 8 Abs. 4 Satz 2 LKRG). Gegenwärtig sind dies ca. 247 000 Datensätze. Eine ähnliche Situation ergibt sich im Fall der Kompromittierung des Schlüssels oder dessen Wechsel aufgrund technologischer oder kryptoanalytischer Fortschritte.

Zur Verfahrensweise bei einem Schlüsselwechsel enthält das LKRG keine Regelungen. Aus den Vorschriften über die Behandlung der eingesetzten Schlüssel lässt sich jedoch entnehmen, dass die Vertrauensstelle nicht über die Möglichkeit verfügen soll, Identitätsdaten selbständig ohne Einschaltung des LDI zu entschlüsseln (§ 8 Abs. 4 Satz 2 2. Halbsatz LKRG). Die damit einhergehenden Missbrauchsmöglichkeiten würden dem Zweck, eine Zuordnung von Identitätsdaten zu Registereintragungen ausschließlich in bestimmten Fällen und unter Beteiligung Dritter zu ermöglichen, zuwiderlaufen. So liefert der Gesamtbestand der Identitätsdaten – neben der Kenntnis der im Krebsregister aufgenommenen Personen – über die Neubildung der Kontrollnummern die Möglichkeit der Zuordnung zu den epidemiologischen Daten.

Für einen Schlüsselwechsel wurde daher mit dem Krebsregister und dem LDI folgende Verfahrensweise vereinbart.

- Die Entschlüsselung geschieht entsprechend § 9 Abs. 5 LKRG unter Beteiligung des LDI.
- Die Kontrolle des LDI ist für den gesamten Zeitraum der Entschlüsselung zu gewährleisten; erforderlichenfalls werden die genutzten Räumlichkeiten während der Programmlaufzeit versiegelt.
- Die erneute Verschlüsselung erfolgt in den Räumlichkeiten der Vertrauensstelle zum frühestmöglichen Zeitpunkt, ebenfalls unter Beteiligung des LDI. Soweit den Umständen nach erforderlich, werden die unverschlüsselten Identitätsdaten bis zur erneuten Verschlüsselung durch den LDI geschützt gegenüber einem Zugriff Dritter verwahrt. Nach erfolgter Verschlüsselung wird der Datenträger mit den Klartextdaten im Beisein von Vertretern des LDI gelöscht.
- Die Vorgänge im Rahmen Entschlüsselung und Neuverschlüsselung sind mit Ort, Zeitpunkt, Zahl der betroffenen Datensätze und etwaiger Vorkommnisse nachvollziehbar zu dokumentieren.

Der anstehende Schlüsselwechsel wurde nach der beschriebenen Verfahrensweise vorgenommen.

21.2.11 E-Mail-Kommunikation im Bereich der Kreisverwaltungen

Die Kommunikation per E-Mail kommt im Bereich der öffentlichen Verwaltung zunehmend zum Einsatz. Insbesondere der Informationsaustausch zwischen verschiedenen Verwaltungen ist hier zu nennen.

Soweit es sich bei den Kommunikationsinhalten um personenbezogene Daten handelt, sind technische und organisatorische Maßnahmen zur Sicherung des Datenschutzes bei der Übertragung erforderlich. Sofern die E-Mail-Kommunikation zwischen den jeweiligen Dienststellen ausschließlich über die Mailserver innerhalb des geschlossenen rlp-Netzes erfolgt, kann i. V. m. den betreiber- und providerseits getroffenen Sicherheitsmaßnahmen für Daten geringer Sensibilität von einem angemessenen Sicherheitsniveau ausgegangen werden. Wenn neben dem rlp-Netz-Anschluss über LDI auch Dienste anderer Netzanbieter zur E-Mail-Kommunikation genutzt werden, ist nicht automatisch von einer vertrauenswürdigen Verbindung auszugehen.

Eine vom LfD durchgeführte Befragung der Kreisverwaltungen ergab, dass überwiegend die elektronische Kommunikation mit anderen Verwaltungen über das rlp-Netz abgewickelt wird. In einigen Fällen erfolgt der E-Mail-Verkehr über sonstige Netzbetreiber.

Grundsätzlich sollte bei der elektronischen Kommunikation darauf geachtet werden, dass bei der Übertragung von personenbezogenen Daten eine Vertraulichkeit – auch gegenüber dem Netzbetreiber – gewahrt wird. Im Rahmen organisatorischer Regelungen (z. B. Dienstanweisung) sollte daher die Übertragung von personenbezogenen Daten nur in verschlüsselter Form erfolgen.

Eine Absicherung gegenüber in E-Mails möglicherweise enthaltenen Schadbestandteilen (Viren) bleibt hiervon unberührt. Derzeit erfolgt am zentralen Mailserver des LDI eine inhaltliche Prüfung der transportierten Mails. Da diese Überprüfung jedoch nur eingeschränkt erfolgen kann, bleibt es weiterhin auch in der Verantwortung der angeschlossenen Verwaltungen, vor Ort für eine entsprechende Sicherheitsinfrastruktur zu sorgen.

21.2.12 Dokumentenverwaltung und -archivierung in der Mittelinstanz (DOMEA)

Im Zusammenhang mit der Erprobung eines Verfahrens zur automatischen Dokumentenverwaltung und -archivierung im Bereich der Mittelinstanz wurde der LfD beteiligt. Die ausgesprochenen Empfehlungen betrafen die Zugriffskontrolle, Recherche, Archivierung und Löschung von Vorgängen sowie eine entsprechende Protokollierung und wurden im Anforderungskatalog berücksichtigt.

Neben der eigentlichen Anwendung sind datenschutzrechtlich deren Betrieb innerhalb der IT-Struktur der jeweiligen Verwaltung sowie die elektronische Kommunikation verschiedener Stellen im Rahmen der Vorgangsbearbeitung und -verwaltung von Bedeutung. Die hierzu im Sicherheitskonzept des Verfahrens genannten Maßnahmenvorschläge tragen den datenschutzrechtlichen Anforderungen ausreichend Rechnung.

Die zunächst pilotweise eingesetzte Lösung soll einheitlich für den Bereich der Landesverwaltung vorgegeben werden. Über eine zentrale oder dezentrale Datenhaltung bei der Verarbeitung und Archivierung von Vorgängen soll auf der Grundlage von Pilotanwendungen entschieden werden. Im weiteren Verlauf des Verfahrens sind örtliche Feststellungen, insbesondere hinsichtlich der Umsetzung der Vorgaben im jeweiligen Betriebskonzept, vorgesehen.

21.2.13 Kfz-Zulassungsverfahren

Im Rahmen der Weiterentwicklung wird derzeit vom LDI das dezentrale landeseinheitliche Kfz-Zulassungsverfahren in ein zentrales Verfahren auf Basis von ASP-Technologie umgewandelt. Ziel dieser Vorgehensweise ist die Bereitstellung des Verfahrens auf Basis von Internettechnologie für die beteiligten Kfz-Zulassungsstellen. Die Datenhaltung erfolgt zentral auf Datenbankservern des LDI, Zugriffe der Verwaltung erfolgen über das Landesdatennetz. Im Zuge der Weiterentwicklung wurde der LfD frühzeitig in die Planung eingebunden. Empfehlungen wurden insbesondere bezüglich der Absicherung der Datenbestände der einzelnen Kfz-Zulassungsbehörden gegeneinander, der Änderung in für das Verfahren von zentraler Bedeutung stehenden Daten sowie der Protokollierung bei Zugriff auf Datenbestände der Kfz-Zulassungsbehörden durch den LDI als verfahrensbetreibende Stelle ausgesprochen. Der LDI hat die Umsetzung dieser Empfehlungen zugesichert. Der LfD wird die Weiterentwicklung des Verfahrens verfolgen und im Rahmen örtlicher Feststellungen überprüfen.

21.2.14 Integriertes rheinland-pfälzisches Mittelbewirtschaftungs- und Auszahlungsverfahren (IRMA)

Im Zusammenhang mit der Einführung des Verfahrens IRMA im nachgeordneten Bereich der Landesverwaltung waren die Abfrage- und Auswertungsmöglichkeiten des Verfahrens Gegenstand einer datenschutzrechtlichen Kontrolle.

Das Verfahren stellt häufig benötigte Abfragemöglichkeiten in Form von Standardauswertungen zur Verfügung. Die einzelnen Auswertungsfunktionen können einzelnen Benutzern oder Benutzergruppen explizit zugewiesen werden. Art und Umfang der Abfragen lassen sich nach der dienstlichen Aufgabenstellung differenzieren. Daneben bietet das Verfahren IRMA die Möglichkeit, Abfragen nach frei wählbaren Gesichtspunkten durchzuführen. Voraussetzung ist auch hier, dass entsprechende Zugriffsrechte auf die Funktion eingerichtet werden. Auch im Fall freier Abfragemöglichkeiten ist der auswertbare Datenbestand auf den dem jeweiligen Benutzer zugewiesenen Umfang beschränkt. Die vorhandenen Möglichkeiten der Zugriffskontrolle hat der LfD hinsichtlich § 9 Abs. 2 Nr. 3 LDSG als ausreichend erachtet.

Allerdings war erkennbar, dass diese bei den Dienststellen nicht im wünschenswerten Umfang bekannt waren. Der LfD hat daher das Finanzministerium als verfahrensbetreuende Stelle gebeten, über die bestehenden Konfigurationsmöglichkeiten in geeigneter Weise zu unterrichten.

Als unzureichend hat der LfD die gegenwärtige Protokollierung im Verfahren IRMA beurteilt. Im Rahmen der Entwicklung des Verfahrens hatte er darauf hingewiesen, dass die Protokollierung von Auswertungen Teil eines angemessenen Datenschutzkonzepts sei. In der Konzeption des Verfahrens wurden daraufhin entsprechende Funktionen vorgesehen. Die Kontrolle hat ergeben, dass entgegen diesen Planungen die Protokollierungsfunktionen nicht realisiert wurden. Auswertungen personenbezogener Daten sind damit nicht im erforderlichen Umfang nachvollziehbar. Der LfD hat den Verfahrensmangel daraufhin als Verstoß gegen die Verarbeitungskontrolle (§ 9 Abs. 2 Nr. 10 LDSG) beanstandet.

Für das gegenwärtige Verfahren ist eine Nachfolgelösung vorgesehen, mit deren Entwicklung ab 2004 begonnen werden soll. Angesichts dessen und mit Blick auf den damit verbundenen Aufwand hat der LfD davon abgesehen, für das laufende Verfahren die nachträgliche Implementierung der ausstehenden Protokollfunktionen zu fordern. Für den Übergangszeitraum soll stattdessen die Möglichkeit freier Abfragen nicht pauschal, sondern nur bei konkretem Bedarf zugewiesen und die Zahl der solcherart Zugriffsberechtigten beschränkt werden. Für die IRMA-Nachfolgelösung ist jedoch eine angemessene Nachvollziehbarkeit personenbezogener Abfragen und Auswertungen sicherzustellen. Das Finanzministerium hat zugesagt, dies bei der technischen Umsetzung zu berücksichtigen.

21.2.15 Fernwartung im Verfahren POLIS.net

Für das von der Polizei betriebene Verfahren POLIS.net fanden im Rahmen des Betriebs bedarfsweise Zugriffe im Rahmen einer Fernwartung statt. Diese erstreckt sich auf den technischen Betrieb der eingesetzten Systeme und umfasst nicht die Betreuung der Datenbank- und Anwendungssoftware.

Hinsichtlich der Festlegung des Zugriffsumfangs im Einzelnen hat der LfD empfohlen, je nach Eingriffstiefe unterschiedliche Wartungsstufen vorzusehen; dem wurde entsprochen. Die Regelungen zur vorherigen Abstimmung und Freischaltung sowie zum Verbindungsaufbau berücksichtigen ebenfalls die Empfehlungen des LfD und begegnen keinen datenschutzrechtlichen Bedenken. So erfolgt u. a. eine Verschlüsselung der Kommunikation zwischen fernwartender Stelle und betroffenem System.

Von Bedeutung war aus Sicht des LfD weiterhin die Kontrolle der durchgeführten Fernwartungsarbeiten. Als vorbeugende Sicherungsmaßnahme und für eine nachträgliche Klärung in Zweifelsfällen hat er daher eine Protokollierung für erforderlich gehalten, anhand derer die durchgeführten Arbeiten konkret nachvollzogen werden können. Das Fernwartungskonzept sieht hierzu vor, dass die Vorgänge der Fernwartung in einer Logdatei dokumentiert werden.

Im Blick auf die Zuverlässigkeit der mit den Wartungsarbeiten betrauten Personen ist neben einer Abfrage der polizeilichen Informations- und Auskunftssysteme die Verpflichtung auf das Datengeheimnis nach § 8 LDSG vorgesehen. Da es sich bei den Auftragnehmern um nichtöffentliche Stellen handelt, hat der LfD empfohlen, ergänzend eine Verpflichtung nach dem Verpflichtungsgesetz vorzunehmen, um die Anwendbarkeit strafrechtlicher Bestimmungen wie bei Amtsträgern zu gewährleisten.

21.2.16 Mobiler Zugang zum Zentralen Verkehrsinformationssystem des Kraftfahrtbundesamtes ZEVIS

Im Rahmen der Erweiterung technischer Zugangsmöglichkeiten auf polizeiliche Anwendungen erprobt die Polizei die Möglichkeiten des Einsatzes mobiler Endgeräte für den Zugriff auf das Zentrale Verkehrsinformationssystem ZEVIS über das Kommunikationsnetz der Polizei. Im Endausbau ist der Einsatz von 750 Systemen im Streifendienst vorgesehen. Verwendet werden handelsübliche, mit einer entsprechenden Client-Software ausgestattete so genannte Handheld-PCs.

Seitens des LfD wurde darauf hingewiesen, dass als Maßstab für die Anbindung mobiler Endgeräte an das Kommunikationsnetz der Polizei bzw. an polizeiliche Anwendungen die Vorkehrungen des gesicherten Wählzugangs zum rlp-Netz zugrunde gelegt werden sollten. Neben der Verschlüsselung der Kommunikation betrifft dies die verlässliche Authentisierung der beteiligten Systeme.

Die pilotweise eingesetzten Lösungen tragen dem Rechnung. So erfolgt eine SSL 128 Bit-Verschlüsselung für die Absicherung der Funkkommunikation und es werden neben einer eindeutigen Geräte-ID benutzerspezifische Schlüssel verwendet. Weiterhin wurde die standardmäßig vorhandene Software für die Verbindung zu den Einwahlknoten durch eine BSI-zertifizierte Lösung ersetzt, die eine Verbindungsaufnahme nur zu festgelegten Systemen und Verfahren zulässt.

21.2.17 Protokollierungskonzept in POLADIS.net

Im Rahmen der technischen Vereinheitlichung polizeilicher Anwendungen ist auch die Neugestaltung des polizeilichen Vorgangsbearbeitungs- und Verwaltungsverfahrens POLADIS erfolgt (vgl. Tz. 5.11.1). Der Funktionsumfang, das Datenmodell und die Rollenstruktur des bisherigen Verfahrens wurden dabei weitgehend übernommen. Vor dem Hintergrund bestimmter Probleme in einem Teil der Vorgängerverfahren bildete die Protokollierung dabei einen Schwerpunkt der datenschutzrechtlichen Begleitung durch den LfD. Die Vorgängerlösung hat Zugriffe schematisch, d. h. ohne logische Abhängigkeiten protokolliert. Dadurch wurden Protokolleinträge ohne zusätzlichen Informationsgehalt erzeugt, die in Einzelfällen zu umfangreichen Datenvolumina geführt haben. Aufgrund der veränderten Verfahrenskonzeption ist dies bei POLADIS.net nicht der Fall.

Verzichtbar war aus Sicht des LfD auch die Protokollierung ergebnisloser Abfragen, es sei denn, ihnen lägen entsprechende Zugriffsbeschränkungen zugrunde. Auch Masken- oder Funktionsaufrufe, die lediglich der Navigation innerhalb der Anwendung dienen und keine personenbezogenen Daten anzeigen oder verarbeiten, waren aus Sicht des Datenschutzes für die Protokollierung ebenfalls ohne Bedeutung.

Den Anforderungen des LfD an eine angemessene Nachvollziehbarkeit der Verarbeitung i. S. des § 9 Abs. 2 Nr. 5 und 10 LDSG wurde weitgehend entsprochen. Die nunmehr vorgesehene, grundsätzlich vollständige Protokollierung ist aus datenschutzrechtlicher Sicht zu begrüßen.

21.2.18 Testbetrieb mit Echtdaten im Verfahren POLADIS.net

Im Rahmen der Weiterentwicklung des Verfahrens war vorgesehen, den entwickelnden Firmen Echtdaten aus dem Wirkbetrieb zur Verfügung zu stellen. Aus datenschutzrechtlicher Sicht stellt die Bereitstellung sensitiver, personenbezogener Daten aus der polizeilichen Arbeit an nichtöffentlichen Stellen eine besondere Situation mit Ausnahmecharakter dar. Im Rahmen der Verfahrensentwicklung sind vorgesehene Tests grundsätzlich anhand geeigneter Testdaten durchzuführen. Die Verwendung von Originaldaten kommt nur in besonderen Fällen und auf der Grundlage angemessener Sicherungsmaßnahmen in Betracht.

Im vorliegenden Fall sollte die Bereitstellung von Vorgangsdaten dazu dienen, die korrekte Übernahme der Daten in das Nachfolgeverfahren sicherzustellen. Im Blick auf die Vielfalt der möglichen Ausprägungen und die neben den Inhaltsdaten erforderliche Übernahme von Metadaten aus der Geschäftskontrolle hat sich der LfD der Auffassung des Ministeriums des Innern und für Sport angeschlossen, dass eine verlässliche Einschätzung der korrekten Datenmigration einen Probelauf mit Echtdaten aus dem laufenden Betrieb erfordert. Aus datenschutzrechtlicher Sicht war hinsichtlich der Metadaten insbesondere von Bedeutung, dass eingestellte Prüf- und Löschfristen sowie Zugriffsregelungen, Sperrungen und vergleichbare Informationen korrekt übernommen werden.

Für die mit den Testarbeiten betrauten Personen war eine Verpflichtung nach § 8 LDSG vorgesehen. Da es sich bei den Auftragnehmern um nichtöffentliche Stellen handelte, hat der LfD empfohlen, ergänzend eine Verpflichtung nach dem Verpflichtungsgesetz vorzunehmen, um die Anwendbarkeit strafrechtlicher Bestimmungen wie bei Amtsträgern zu gewährleisten. Weiterhin sollten jederzeitige Kontrollmöglichkeiten durch den Auftraggeber und den LfD ergänzend als Auftragsbedingung vorgesehen und die Löschung der eingespielten Vorgangsdaten nach Projektende schriftlich bestätigt werden. Den Empfehlungen des LfD wurde entsprochen.

2.3 Allgemeine technisch-organisatorische Aspekte

21.3.1 Einsatz von Open Source Software in der Verwaltung

Der Einsatz von Open Source Software wird seitens der Datenschutzbeauftragten grundsätzlich positiv gesehen. Ein wesentlicher Gesichtspunkt ist dabei die im Gegensatz zu proprietären Lösungen bestehende Möglichkeit, eine Überprüfung des Quellcodes der eingesetzten Programme vornehmen zu können. Open Source Software trägt insoweit der Forderung der Datenschutzbeauftragten nach Transparenz der Datenverarbeitung Rechnung.

Der mit einer Quellcode-Prüfung verbundene Aufwand relativiert in der Praxis zwar die Ausnutzung dieses Transparenzgewinns. Dennoch ermöglicht es das Open Source-Konzept, die Vertrauenswürdigkeit von Software in größerem Umfang überprüfen zu können als bei Lösungen, die auf eine derartige Offenlegung verzichten.

Neben Transparenz und Vertrauenswürdigkeit sind Sicherheitsaspekte von Bedeutung. Auch diese bedürfen jedoch einer differenzierten Betrachtung. Sicherheitsprobleme treten sowohl im Bereich von Open Source Software als auch bei proprietären Lösungen auf. Die vorliegenden Erkenntnisse zeigen, dass Open Source Software vielfach einer intensiveren und teils systematischen Überprüfung auf Schwachstellen unterzogen wird und bei erkannten Sicherheitslücken Softwareaktualisierungen zeitnah bereitgestellt werden. Allerdings haben auch Hersteller proprietärer Software die Bedeutung sicherer Software erkannt und entsprechende Schritte unternommen.

Die eingangs genannte Transparenz der eingesetzten Software eröffnet unter Sicherheitsaspekten auch Angriffsflächen. Open Source-Lösungen sind damit nicht a priori sicherer als andere Lösungen. Der Open Source-Ansatz ermöglicht es dem Anwender jedoch, die Sicherheit von IT-Lösungen selbst zu bestimmen und ggf. anzupassen.

Aus Sicht des LfD hat das Open Source-Konzept datenschutzrechtliche Vorteile; ein verstärkter Einsatz von Open Source Software im Bereich der Landesverwaltung ist daher zu begrüßen. Eine Entscheidung für diese Lösungen führt jedoch nicht automatisch zu datenschutzgerechten Verfahren. Die diesbezüglichen Anforderungen betreffen Open Source und proprietäre Software gleichermaßen.

21.3.2 Elektronische Signatur in der Landesverwaltung

Vor dem Hintergrund der im Jahr 2001 erfolgten Novellierung des Signaturgesetzes und der nachfolgenden Änderung bundesgesetzlicher Formvorschriften beabsichtigt die Landesregierung die Einführung einer elektronischen Signaturlösung für die Landesverwaltung. In Zusammenarbeit mit dem LDI soll bis Ende 2003 das chipkartengestützte Signatursystem „rlp-Trust“ an rund 3 600 Arbeitsplätzen innerhalb der Verwaltungen eingesetzt werden.

Die Landesregierung folgt damit u. a. Empfehlungen des LfD, wonach zum Schutz elektronischer Informationen, an die besondere Anforderungen hinsichtlich ihrer Vollständigkeit, Korrektheit oder des Nachweises der Urheberschaft gestellt werden, auf elektronische Signaturverfahren zurückgegriffen werden sollte (siehe 18. Tb., Tz. 21.3.2).

Die im Rahmen elektronischer Signaturlösungen erforderliche Infrastruktur kann grundsätzlich auch für die Verschlüsselung sensibler personenbezogener Informationen genutzt werden. Im Blick auf die Bestrebungen, Verwaltungsleistungen künftig auch auf elektronischem Weg, z. B. über das Internet, zu erbringen (E-Government), sind entsprechende Lösungen aus Sicht des LfD unverzichtbar. Sie eröffnen weiterhin Wege, sich bei der Auswahl und Gestaltung von Verfahren datenschutzfreundlicher Technologien zu bedienen. Im Zusammenhang mit dem Einsatz elektronischer Signaturverfahren betrifft dies insbesondere die Möglichkeit, anstelle namentlich zugeordneter Zertifikate Pseudonyme verwenden zu können und damit in geeigneten Fällen auf einen konkreten Personenbezug zunächst zu verzichten (vgl. Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Oktober 1997 zur Erforderlichkeit datenschutzfreundlicher Technologien [17. Tb., Anlage 3]).

Der LfD wird die Einführung und Nutzung elektronischer Signaturlösungen in der Verwaltung auch weiterhin datenschutzrechtlich begleiten.

21.3.3 Empfehlungen zum Einsatz von Verschlüsselungsverfahren

Zum Einsatz von Verschlüsselungsverfahren hatte der LfD im 17. Tb., Tz. 21.3.10 Stellung genommen. Vor dem Hintergrund der zunehmenden Berücksichtigung entsprechender Lösungen in unterschiedlichen Anwendungsszenarien hat der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum Einsatz kryptografischer Verfahren erstellt. Diese steht im Internet-Angebot des LfD unter www.datenschutz.rlp.de zur Verfügung.

21.3.4 Einsatz des Programms Prettty Good Privacy (PGP) in der Verwaltung

Bei dem Programm PGP handelt es sich um eine für Verschlüsselungs- und Signaturzwecke verbreitet eingesetzte Lösung. Im Blick auf entsprechende Anforderungen im Bereich der Landes- und Kommunalverwaltung wurde der LfD mehrfach gebeten, zur Einsetzbarkeit von PGP bzw. der vergleichbaren Open Source-Lösung Gnu Privacy Project (GnuPP) Stellung zu nehmen.

Weder PGP noch GnuPP erfüllen die Anforderungen des Signaturgesetzes an eine qualifizierte elektronische Signatur. Für viele Einsatzbereiche ist dies jedoch ohne Bedeutung. Im 18. Tb. (Tz. 21.3.2) hatte der LfD dargestellt, dass in vielen Fällen Lösungen einer fortgeschrittenen elektronischen Signatur im Sinne des § 2 Nr. 2 SigG ausreichend sind. Dem Einsatz von PGP/GnuPP stehen insoweit datenschutzrechtliche Bedenken nicht entgegen.

Vor einem etwaigen Einsatz von PGP sollten hinsichtlich der Schlüsselverwaltung folgende Punkte geklärt werden:

- die Festlegung von Algorithmen und Schlüssellängen,
- die Verwendung von Individual- bzw. Gruppenschlüsseln,
- die Art der Schlüsselerzeugung (zentral oder dezentral),
- die Notwendigkeit, im Bedarfsfall auf Kopien der eingesetzten geheimen Schlüssel zurückgreifen zu können,
- die ggf. erforderliche Zertifizierung der öffentlichen Schlüssel,
- die Gültigkeit der verwendeten Schlüssel sowie
- das Verfahren der Sperrung von Schlüsseln im Fall der Kompromittierung, des Verlusts oder des Ausscheidens von Schlüsselinhabern.

21.3.5 Schlüsselverwaltung bei elektronischer Signatur und Verschlüsselung

Im Blick auf den zunehmenden Einsatz kryptografischer Verfahren wurde der LfD verschiedentlich zur Schlüsselverwaltung, insbesondere zur Frage der Verwendung von Gruppen- bzw. Dienststellenschlüsseln um Stellungnahme gebeten.

Gegen die Nutzung von Gruppen- oder Dienststellenschlüsseln bestehen aus datenschutzrechtlicher Sicht keine Bedenken, wenn lediglich die Zurechenbarkeit zu einer Behörde oder Organisationseinheit erforderlich ist. Gleiches gilt im Fall der Verschlüsselung, soweit lediglich die Übertragung personenbezogener Daten gegenüber einer Kenntnisnahme Dritter außerhalb der beteiligten Stellen abgesichert werden soll.

Soweit eine elektronische Signatur jedoch einer bestimmten natürlichen Person verbindlich zugerechnet werden soll, bzw. eine Entschlüsselung nur einer bestimmten Person möglich sein soll, muss der verwendete Schlüssel eindeutig sein. Insoweit empfiehlt es sich, separate Schlüsselpaare für Signatur und Verschlüsselung zu verwenden.

Die Anfertigung von Sicherungskopien oder die Berücksichtigung von Wiederherstellungsmöglichkeiten, als Vorsorge gegen Verlust oder Beschädigung, begegnet, soweit die genannten Einschränkungen bei Dienststellen- oder Gruppenschlüsseln beachtet werden, keinen Bedenken.

21.3.6 Gewährung von Akteneinsicht in Form digitalisierter Zweitakten

Im Zusammenhang mit der Abwicklung eines Großverfahrens wurde der LfD um Stellungnahme zu der Möglichkeit gebeten, Akteneinsicht in Form von auf CD-ROM bereitgestellter digitalisierter Aktenkopien zu gewähren.

Für das visuelle Erscheinungsbild einer Aktenkopie bedeutet es keinen Unterschied, ob sie auf einem Kopiergerät oder mit einem Scanner erzeugt wurde. Wird die Grafikdatei ausgedruckt, entspricht sie auch hinsichtlich ihrer Verkörperung einer Papierkopie.

Wenn im Rahmen der Akteneinsicht die Anfertigung von Papierkopien zulässig ist, gilt dies aus datenschutzrechtlicher Sicht damit im Grundsatz auch für digitalisierte Zweitakten in Form von Bitmap-Dateien. Eine andere Beurteilung ergäbe sich möglicherweise dann, wenn – für Textdokumente – beim Scannen OCR-Daten erzeugt würden, die zwar inhaltlich, aber nicht optisch mit dem Original übereinstimmen. Hier dürfte der Vergleich mit einer Abschrift zu ziehen sein. In Fällen, in denen Zweitakten üblicherweise mit einer eindeutigen Kennzeichnung versehen werden, um ihren Verbleib nachzuweisen, wäre dies auch für ihre digitalisierte Form vorzusehen. Geeignete technische Möglichkeiten stehen zur Verfügung. Datenschutzrechtliche Vorteile ergeben sich bei der Überlassung auf CD-ROM dadurch, dass die Imagedateien verschlüsselt, durch Passworte gesichert oder mit Prüfsummen bzw. Signaturen versehen werden können, und damit eine im Einzelfall notwendige besondere Vertraulichkeit oder Integritätssicherung technisch gewährleistet werden kann.

Soweit eine ausreichende Sorgfalt bei Aufbewahrung und Weitergabe der Datenträger gewahrt wird und im Übrigen eine den Papierkopien entsprechende Behandlung erfolgt, kann aus datenschutzrechtlicher Sicht Akteneinsicht auch in Form digitalisierter Aktenkopien gewährt werden.

21.3.7 Steuerung und Kontrolle des IT-Einsatzes im kommunalen Bereich

Im Rahmen einer durchgeführten örtlichen Feststellung zum technisch-organisatorischen Datenschutz bei einer Verbandsgemeindeverwaltung wurde bekannt, dass die Verwaltung den überwiegenden Teil der Betreuung der IT-Infrastruktur durch ein externes privatwirtschaftlich organisiertes Unternehmen durchführen lässt. Zwar befinden sich die Hardwarekomponenten wie auch die gespeicherten Informationen ausschließlich in Räumen der Verbandsgemeindeverwaltung, der tatsächliche Zugriff auf diese Daten ist jedoch durch das dienstleistende Unternehmen durch Fernzugriffe – auch ohne Kenntnisnahme der Verwaltung – jederzeit möglich. Dieser Umstand ist aus datenschutzrechtlicher Sicht als äußerst bedenklich zu bewerten, zumal die den Dienstleistungen zugrunde liegenden vertraglichen Regelungen nur unzureichende Dokumentationspflichten seitens des Dienstleisters wie auch unzureichende Kontrollmöglichkeiten seitens der Verwaltung als Auftraggeberin enthalten. Da sich im konkreten Fall durch die andauernde Praxis dieser externen Betreuung ein regelrechtes Abhängigkeitsverhältnis aufgebaut hat, ist die Verwaltung nicht mehr in der Lage, aus eigener Kraft die Grundbetreuung der IT-Infrastruktur sicherzustellen. Der LfD wird dies als Verstoß gegen datenschutzrechtliche Bestimmungen beanstanden.

21.3.8 Speicherung und Weitergabe der Protokolldaten von Webservern

Das „World Wide Web“ (WWW) ist mehr denn je eine geeignete Plattform zur Präsentation. Kaum eine Verwaltung in Rheinland-Pfalz nutzt nicht dieses Medium zur Darstellung und Information im Internet. Verständlich hierbei ist, dass die Anbieter von Informationen im WWW das Nutzungsverhalten derer, die ihre Seiten besuchen, gerne analysieren möchten. Protokolldateien, wie sie beim Betrieb von Webservern anfallen, sind hierzu geeignet, jedoch ergibt sich bei deren Auswertung ein datenschutzrelevanter Aspekt. Die Logdateien enthalten zum Teil personenbezogene oder zumindest personenbeziehbare Daten. Neben der IP-Adresse der beteiligten Rechner können in den protokollierten Informationen auch Namen, Bankverbindungen, Kennwörter und andere Informationen enthalten sein, die sicherlich für eine statistische Auswertung des Nutzungsverhaltens entbehrlich sind.

Insbesondere wenn die Auswertung der Logdateien durch Dritte erfolgen soll, ist es aus Sicht des LfD erforderlich, die Informationen hinreichend zu anonymisieren. Entsprechende Hinweise zur Behandlung von Webserverlogdateien vor der Weitergabe an Dritte zur Auswertung sind auf der Internetseite des LfD veröffentlicht worden.

21.3.9 Voice-over-IP (VoIP) in der Landesverwaltung

Seitens verschiedener Bereiche der Landesverwaltung ist eine Integration der Sprachkommunikation in die bestehende Dateninfrastruktur mittels VoIP angedacht. Beim Einsatz von VoIP wird Sprache – wie andere Daten auch – in Form von IP-Paketen durch Netze transportiert. Hierbei ist sicherzustellen, dass die Transportwege der „Sprachdaten“ ebenso abgesichert sind, wie dies für andere Daten der Fall ist.

Generell ist hierbei zu unterscheiden, ob ein im rlp-Netz als VoIP-Verbindung geführtes Telefonat auch außerhalb des rlp-Netzes über VoIP, d. h. über das Internet, weitergeführt wird oder ob mittels Gateway eine Einspeisung in ein anderes öffentliches Telefonnetz (z. B. ISDN) erfolgen soll. Sofern die VoIP-Kommunikation auf das rlp-Netz beschränkt bleibt, ist keine unmittelbare „Gefährdung“ des rlp-Netzes (oder eines VPN) durch schadensfunktiontragende VoIP-Pakete aus dem Internet zu erwarten. Wird zum Zwecke der VoIP-Kommunikation ein Verbindungsweg zwischen dem öffentlichen Netz (Internet) und dem rlp-Netz eröffnet, ist sicherzustellen, dass die Kommunikation ausschließlich über eine geeignete Sicherheitsinfrastruktur abgewickelt wird.

Die derzeitigen Planungen in den einzelnen Verwaltungsbereichen sehen zunächst lediglich den Einsatz von VoIP als interne Lösung zur Kommunikation vor, so dass keine Anbindung an öffentliche Netze erfolgt. Gleichwohl ist davon auszugehen, dass in Zukunft auch öffentliche Kommunikationsnetze zum Transport von Sprachinformationen über VoIP genutzt werden. Der LfD wird die Entwicklung in diesem Bereich weiter beobachten.

21.3.10 IT-Sicherheitsleitlinien für die Landesverwaltung

Die zunehmende Abhängigkeit der Verwaltungen von der eingesetzten Informationstechnik, die steigende Nutzung des Internets als Informationsplattform und die aus Sicherheitsvorfällen resultierenden Beeinträchtigungen führen – zumal im Blick auf den erklärten Ausbau von E-Government-Lösungen – zu grundlegenden Fragen des Schutzes und der Sicherheit von Informationen. Die IT-Sicherheit der Kommunikationsstrukturen und der Datenbestände der öffentlichen Verwaltung ist auch aus Sicht der Landesregierung von zunehmend hoher Bedeutung (vgl. Landtagsdrucksache 14/1459).

Unter Mitarbeit des LfD hat daher eine Arbeitsgruppe des IT-Ausschusses der Landesregierung Leitlinien zur Sicherheit beim Einsatz der Informationstechnik in der Landesverwaltung formuliert. Diese fußen auf dem IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Sicherheitsleitlinien wurden im Ministerrat beschlossen und als Rundschreiben der Landesregierung veröffentlicht (Planung und Realisierung der IT-Sicherheit in der Landesverwaltung Rheinland-Pfalz, MinBl. vom 4. Juni 2003). Sie erlegen den Verwaltungen bestimmte organisatorische und technische Vorkehrungen auf. Folgende Kernpunkte sind aus Sicht des LfD darin von besonderer Bedeutung:

– Grundlage IT-Grundschutzhandbuch

Die Behörden, Gerichte und sonstigen Stellen der Landesverwaltung haben das IT-Grundschutzhandbuch des BSI anzuwenden. Dieser weithin akzeptierte und regelmäßig aktualisierte Sicherheitsleitfaden deckt mit seinen Gefährdungs- und Maßnahmenkatalogen die Sicherheitsbedürfnisse der meisten Verwaltungen weitgehend ab.

– Benennung einer für IT-Sicherheit verantwortlichen Stelle

Jede Verwaltung ist für die Umsetzung ihrer Sicherheitsziele verantwortlich. Die Analyse des jeweiligen Schutzbedarfs sowie Auswahl und Umsetzung geeigneter Maßnahmen liegen in lokaler Verantwortung. Für jede Verwaltung ist eine verantwortliche Stelle zu benennen, die bei sicherheitsrelevanten Ereignissen zu informieren ist und die erforderlichen Maßnahmen koordiniert. Die Verfahrensweise bei sicherheitsrelevanten Vorkommnissen ist festzulegen. Die übergreifende IT-Sicherheit wird innerhalb des Geschäftsbereichs durch das jeweilige Ministerium koordiniert, ressortübergreifende Fragen durch das für allgemeine IT-Angelegenheiten der Landesverwaltung zuständige Ministerium – gegenwärtig ist dies das Innenministerium.

– Schutzbedarfsanalyse und Sicherheitskonzept

Die vorhandene IT-Struktur einer Verwaltung und die eingesetzten Verfahren sind zu erfassen und hinsichtlich ihres Schutzbedarfs zu überprüfen. Zum Schutz aufgabenkritischer Komponenten sind geeignete Maßnahmen auszuwählen und in einem Sicherheitskonzept darzustellen. Die Sicherheitsmaßnahmen müssen gewährleisten, dass der ordnungsgemäße Betrieb von IT-Systemen, die Vollständigkeit, Korrektheit und Vertraulichkeit von Informationen angemessen vor Beeinträchtigungen geschützt sind.

– Kryptografische Verschlüsselung

Es ist zu gewährleisten, dass bei Bedarf Informationen durch kryptografische Verschlüsselung auch innerhalb der Verwaltung, z. B. gegenüber Personen mit besonderen Zugriffsrechten auf den eingesetzten IT-Systemen, vertraulich gehalten werden können. Gleiches gilt für Informationen, die in elektronischer Form an Dritte weitergegeben oder von Dritten empfangen werden und vor unbefugter Kenntnisnahme zu schützen sind.

– Elektronische Signatur

Es muss gewährleistet sein, dass für den Schutz von Informationen, an die besondere Anforderungen hinsichtlich ihrer Vollständigkeit, Korrektheit oder des Nachweises der Urheberschaft gestellt werden, bei Bedarf die Verwendung einer elektronischen Signatur möglich ist.

– Verfügbarkeit relevanter Informationen

Für die Wahrnehmung von Sicherheitsaufgaben wird im Intranet des Landes eine „Informationsplattform IT-Sicherheit“ aufgebaut.

Über die Umsetzung der Leitlinien ist im IT-Ausschuss zu berichten. Der LfD begrüßt ausdrücklich, dass nach längerer Vorarbeit die Sicherheitsleitlinien nunmehr in der vorliegenden Form verabschiedet wurden. Die Erkenntnisse aus seiner Kontroll- und Beratungstätigkeit haben gezeigt, dass es häufig weniger um die Frage geht, welche Maßnahmen konkret zu treffen wären, als darum, IT-Sicherheit als notwendigen Bestandteil des IT-Einsatzes gedanklich, technisch und organisatorisch zu verankern. Dies wird mit den vorliegenden Leitlinien unterstützt. Sie erlauben es, Ergebnisse einzufordern und damit einen zwar allmählichen, aber stetigen Sicherheitsprozess zu initiieren.

21.4 Der behördliche Datenschutzbeauftragte

Gemäß § 11 LDSG haben öffentliche Stellen, bei denen mindestens zehn Beschäftigte regelmäßig personenbezogene Daten verarbeiten, schriftlich einen behördlichen Datenschutzbeauftragten (behDSB) zu bestellen. Dieser muss die erforderliche Sachkunde und Zuverlässigkeit besitzen.

Mit der Bestellung eines behDSB soll gewährleistet werden, dass eine „Datenschutzfachkraft vor Ort“ die öffentliche Stelle bei der Umsetzung der komplexen Materie des Datenschutzes unterstützt und berät. Nach der Intention des Gesetzgebers soll der behDSB innerhalb der Verwaltung die zentrale Anlaufstelle in allen Datenschutzfragen und Koordinator für alle Datenschutzmaßnahmen sein. Unter dem Aspekt der erforderlichen Sachkunde ist mit der Novellierung des LDSG die Möglichkeit geschaffen worden, Personen außerhalb der verantwortlichen Stelle oder mit Zustimmung der zuständigen Aufsichtsbehörde auch Bedienstete anderer öffentlicher Stellen als behDSB zu bestellen. Sachliche Gesichtspunkte sprechen jedoch dafür, den behDSB aus den eigenen Reihen zu rekrutieren.

Die Aufgaben und Befugnisse eines behDSB sind in § 11 Abs. 3 LDSG festgelegt. Die Festlegung ist jedoch nicht abschließend – vielmehr bleibt es der jeweiligen verantwortlichen Stelle überlassen, ihm weitere Aufgaben zu übertragen.

Insbesondere hinsichtlich der erforderlichen Sachkunde und Zuverlässigkeit sowie der Aufgaben eines behDSB können aus den vom LfD herausgegebenen „Hinweisen zum behördlichen Datenschutzbeauftragten“ weitere Informationen entnommen werden. Diese sind auch unter der Rubrik Materialien im Internetangebot des LfD (www.datenschutz.rlp.de) abrufbar.

21.5 Datenschutzregister/Verfahrensverzeichnis

Nach § 27 Abs. 1 LDSG haben die verantwortlichen Stellen Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, zur Eintragung in das beim LfD geführte Datenschutzregister anzumelden. Es handelt sich dabei nicht um ein Genehmigungs- oder Freigabeverfahren. Für den LfD bilden diese Anmeldungen eine wichtige Grundlage der Kontrollarbeit. Darüber hinaus kann der behördliche Datenschutzbeauftragte den Anmeldungen die Informationen entnehmen, die er für die Wahrnehmung seiner Aufgaben nach § 11 LDSG benötigt. Der LfD hat den bislang vorhandenen Vordruck den Anforderungen des novellierten LDSG angepasst.

Wie in der Vergangenheit ist auch in diesem Berichtszeitraum immer wieder festzustellen, dass die Anmeldungen zum Datenschutzregister nicht oder nicht rechtzeitig erfolgten. Es ist auch festzustellen, dass die Zahl der Anmeldungen rückläufig ist – statt dessen steigt die Zahl der Änderungen oder Ablösungen von bereits eingesetzten Verfahren, insbesondere vor dem Hintergrund des Einsatzes neuer Techniken.

Gemäß § 11 Abs. 2 LDSG haben die verantwortlichen Stellen ein Verzeichnis der Verfahren zu führen, in denen personenbezogene Daten automatisiert verarbeitet werden (Verfahrensverzeichnis). Innerhalb der verantwortlichen Stelle ist hierfür grundsätzlich der behördliche Datenschutzbeauftragte zuständig (§ 11 Abs. 3 Nr. 4 LDSG).

Die Bestimmungen zum Verfahrensverzeichnis und zur Anmeldung zum Datenschutzregister zielen auf die Herstellung von Transparenz sowohl innerhalb wie außerhalb der verantwortlichen Stelle. Das Verfahrensverzeichnis ist weiterhin ein Hilfsmittel der Auskunftserteilung (§ 18 LDSG), denn es enthält Angaben darüber, wo in der Verwaltung personenbezogene Daten in automatisierten Verfahren verarbeitet werden.

Im Rahmen der Anmeldung zum Datenschutzregister ist dem LfD auch eine Verfahrensbeschreibung nach § 10 Abs. 2 LDSG vorzulegen. Somit sollte das vor Ort geführte Verfahrensverzeichnis mit den beim LfD angemeldeten Verfahren übereinstimmen.

Weitere Informationen können aus der vom LfD herausgegebenen „Orientierungshilfe zur Führung des Verfahrensverzeichnisses und zur Anmeldung zum Datenschutzregister“ entnommen werden, die ebenfalls in seinem Internetangebot unter www.datenschutz.rlp.de unter der Rubrik Materialien abrufbar ist.

22. Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen

22.1 Öffentlich-rechtliche Wettbewerbsunternehmen

22.1.1 Datenerhebung zur Fehlbelegungsabgabe

Eine Wohnungsbaugesellschaft verlangte im Rahmen von Mieterhöhungsbegehren die Vorlage von Fehlbelegungsbescheiden ihrer Mieter.

Hierzu vertrat der LfD folgende Auffassung: Nach BGB darf eine Mieterhöhung nach Wegfall der öffentlichen Bindung der Wohnung maximal in Höhe der gezahlten Fehlbelegungsabgabe vorgenommen werden. Um dem Vermieter die Festsetzung der neuen Miete zu ermöglichen, kann dieser vom Mieter Auskunft über die Verpflichtung zur Ausgleichszahlung und über deren Höhe verlangen. Dem Vermieter steht jedoch kein genereller Anspruch auf Vorlage von Belegen, insbesondere einer Kopie des Bescheids über die Fehlbelegungsabgabe zu. In diesem Bescheid sind Informationen enthalten, deren Kenntnis für den Vermieter in diesem Zusammenhang nicht erforderlich ist, wie z. B. Angaben über das Einkommen.

Die Wohnungsbaugesellschaft änderte daraufhin ihr Verfahren zur Datenerhebung: Man wies nunmehr ausdrücklich darauf hin, dass alle Informationen außer dem Betrag im Fehlbelegungsbescheid geschwärzt werden können.

22.1.2 Lotto im Internet

Lotto Rheinland-Pfalz bietet die Möglichkeit, auch über das Internet Lotto zu spielen. Dabei nimmt man die Hilfe eines privaten Dienstleisters in Anspruch. Dieser wechselte – mit Genehmigung des Ministeriums der Finanzen – im April 2003 und einige Spieler glaubten nun, dass ihre persönlichen Daten an diesen Dienstleister übermittelt worden waren, so dass sie zukünftig bei diesem ihren Tipp hätten abgeben müssen.

Aus datenschutzrechtlicher Sicht war die Angelegenheit jedoch etwas anders zu beurteilen. Die Spielteilnahme und damit verbunden die Angabe der persönlichen Daten auf der Internetseite von Lotto Rheinland-Pfalz erfolgten freiwillig. Grundlage dieser freiwilligen Angaben waren die Teilnahmebedingungen für das Lotto im Internet, die die Teilnehmer auf der Internetseite aufrufen konnten und durch die Freigabe ihrer Eingaben anerkannten. Aus den Teilnahmebedingungen ergab sich ausdrücklich, welche Funktion der private Dienstleister im Rahmen des Lottospiels übernahm. Auch wurde auf der Internetseite von Lotto Rheinland-Pfalz ausdrücklich darauf hingewiesen, dass dieses Geschäft in Zusammenarbeit mit dem Dienstleister erfolgte. Nach jeder Änderung der Geschäftsbedingungen mussten diese erneut vom Kunden akzeptiert werden. Es war daher nicht von einer unzulässigen Datenübermittlung auszugehen. Vielmehr waren die am Spiel beteiligten Stellen durch die Teilnahmebedingungen hinreichend transparent für den Kunden dargestellt, so dass von einer Datenverarbeitung aufgrund einer informierten Einwilligung auszugehen war.

Bei der Prüfung der Eingaben stellte sich jedoch heraus, dass das Internet-Angebot von Lotto Rheinland-Pfalz nicht den Anforderungen des TDDSG entsprach. Es fand sich kein Hinweis auf die Verarbeitung der Nutzerdaten. Auch wurde nicht darüber informiert, dass man mit Verbringung des Lottoscheins in den Warenkorb auf die Seite eines anderen Anbieters vermittelt wird. Lotto Rheinland-Pfalz überarbeitete daraufhin sein Internet-Angebot.

22.2 Sparkassen

22.2.1 Adressabgleichungen bei der Sparkasse

Eine Petentin wurde plötzlich von einer Bank, bei der sie ein Konto hatte, unter des Adresse ihres Arbeitskollegen geführt. Die Bank hatte die „Adressänderung“ von der Schufa mitgeteilt bekommen.

Die Nachforschungen, an denen auch andere Aufsichtsbehörden beteiligt waren, ergaben Folgendes: Die Petentin unterhielt mit einem Arbeitskollegen ein Sparkonto bei einer Sparkasse. Als sich die Adresse des Arbeitskollegen änderte, wurde dessen neue Adresse der Petentin nicht nur als zweiter Gläubigerin dieses Sparkontos, sondern auch als Inhaberin aller anderen Konten, die diese zum damaligen Zeitpunkt bei der Sparkasse unterhielt, zugeordnet. Hierzu gehörte auch ein Girokonto. Dies hatte wiederum zur Folge, dass die Adressänderung routinemäßig an die Schufa weitergemeldet wurde, die nun ihrerseits die vermeintlich neue Anschrift an die Kreditinstitute weitergab, mit denen die Petentin in Geschäftsbeziehungen stand. Unglücklicherweise kam es ein halbes Jahr später erneut zu einer Panne bei der Sparkasse: Bei einer Adressänderung eines weiteren Kunden wurden die Kontonummern verwechselt, so dass die Petentin wiederum unter einer falschen Adresse geführt wurde. Zudem gab die Sparkasse dieses Mal die vermeintlich neue Adresse an einen Verbundpartner weiter, bei dem die Petentin ebenfalls Kundin war.

Dem Namen der Petentin wurden durch die Sparkasse zweimal falsche Anschriften zugeordnet. Dies stellte einen Eingriff in ihr Persönlichkeitsrecht dar. Die Daten wurden sodann als Folge der unrechtmäßigen Adressänderung an Dritte übermittelt. Dadurch wurde der Grundrechtseingriff intensiviert. Die Daten wurden mittlerweile bei allen Beteiligten berichtigt. Das Vorgehen der Sparkasse war auf Fehler einiger Mitarbeiter zurückzuführen. Diese wurden durch die Sparkasse erneut eindringlich auf den unbedingt erforderlichen sorgfältigen Umgang mit personenbezogenen Daten hingewiesen. Die Sparkasse versicherte, alles zu tun, damit zukünftig solche Fehler vermieden werden können.

22.2.2 Erbeinsetzung durch die Sparkasse

Eine Kreissparkasse hatte einer Petentin Informationen über einen Darlehensvertrag der Sparkasse mit deren verstorbener Schwester mitgeteilt. Die Sparkasse ging davon aus, dass die Petentin Erbin ihrer Schwester war. Zu diesem Zeitpunkt wusste die Petentin jedoch noch nicht, dass der Enkel ihrer Schwester als gesetzlicher Erbe die Erbschaft ausgeschlagen hatte und sie somit als Erbin in Betracht kam. Die Petentin hielt daher das Schreiben der Sparkasse für eine überflüssige Übermittlung personenbezogener Daten ihre Schwester betreffend, da zu diesem Zeitpunkt überhaupt nicht klar gewesen sei, dass sie Erbin werden würde.

Auf datenschutzrechtliche Regelungen können sich jedoch nur lebende natürliche Personen berufen. Da die Schwester der Petentin zurzeit der Datenübermittlung bereits verstorben war, lag in dem Vorgehen der Sparkasse kein datenschutzrechtlich relevanter Sachverhalt.

22.2.3 Schufa-Merkblatt

Eine Petentin legte dem LfD ein Merkblatt der Sparkasse zur Schufa vor mit der Bitte um Überprüfung, ob dies den datenschutzrechtlichen Anforderungen entspreche. Grundsätzlich enthielt das Merkblatt alle notwendigen Informationen zur Schufa, jedoch fehlten Hinweise zum sog. Score-Verfahren. Eine Nachfrage bei der Sparkasse ergab, dass es sich bei dem Merkblatt um ein veraltetes Formular handelte. In den neu aufgelegten Merkblättern waren die geforderten Informationen enthalten. Die Sparkasse sagte zu, alle alten Informationen aus dem Verkehr zu ziehen und zu gewährleisten, dass zukünftig nur noch vollständige Exemplare auf dem neuesten Stand ausgegeben werden.

22.2.4 Schufa-Klausel bei Eröffnung eines Guthabenkontos

Ein Petent wollte bei einer Sparkasse ein Girokonto auf Guthabenbasis eröffnen. Er lehnte es ab, die ihm vorgelegte Schufa-Klausel zu unterzeichnen, also sein Einverständnis zu erteilen, dass die Sparkasse Informationen über die Girokontoeröffnung an die Schufa übermittelt. Er begründete dies damit, dass für die Bank überhaupt kein Kreditrisiko bestehe, da er vertraglich ein reines Guthabenkonto vereinbaren wollte. Die Sparkasse lehnte daraufhin die Kontoeröffnung ab. Auch andere ortsansässige Banken verhielten sich in dieser Weise, so dass sich der Petent schließlich an den LfD wandte. Auf dessen Nachfrage führte die Sparkasse aus, dass bei jeder Art von Girokontoeröffnung das Einverständnis des Kunden dafür eingeholt werde, dass die Kontoverbindungsdaten an die Schufa übermittelt werden.

Ein solches Vorgehen ist datenschutzrechtlich bedenklich: Die Schufa als Schutzgemeinschaft für allgemeine Kreditsicherung dient dazu, Informationen über Kreditabwicklungen zu sammeln und Auskünfte darüber zu geben, um dadurch das Geschäftsrisiko u. a. von Kreditinstituten zu minimieren. Im Fall der Eröffnung eines Guthabenkontos ist ein solches Risiko und damit auch ein berechtigtes Interesse der Kreditinstitute an einer entsprechenden Datenübermittlung nicht zu erkennen. Etwas anderes gilt nur, wenn die Betroffenen in eine solche Übermittlung eingewilligt haben. Die Einwilligung muss jedoch auf freiwilliger Basis erfolgen. Die Verweigerung der Einwilligung wird aber in der Regel die Versagung eines Girokontos zur Folge haben. Wenn alle Banken in dieser Weise verfahren, wird der Betroffene keine Möglichkeit haben, ein Girokonto zu eröffnen. Ein Girokonto ist aber mittlerweile nahezu unverzichtbar, um am wirtschaftlichen Leben teilnehmen zu können. Es war folglich davon auszugehen, dass die Einwilligungserklärung zur Datenübermittlung an die Schufa bei Eröffnung eines Guthabenkontos nicht als freiwillig im Sinne des Datenschutzrechts einzuordnen ist.

Der LfD bat die Sparkasse, die Verfahrensweise zukünftig datenschutzgerecht zu gestalten. Das Kreditinstitut sagte ein entsprechendes Vorgehen zu.

23. Sonstiges

23.1 Datenschutz bei der Beantwortung parlamentarischer Anfragen

Im Rahmen seiner Beratungsaufgabe hatte der LfD gegenüber dem Direktor beim Landtag zu der Frage Stellung zu nehmen, ob der Landtagsverwaltung bei der Veröffentlichung von Antworten der Landesregierung auf parlamentarische Anfragen ein eigenständiges Prüfungsrecht im Hinblick auf deren datenschutzrechtliche Zulässigkeit zusteht.

Im Ergebnis hielt der LfD auf der Grundlage des § 5 Abs. 1 DSO-LT eine eigene Prüfungsbefugnis der Landtagsverwaltung für gegeben.

Gemäß Art. 4 a Abs. 1 LV hat jeder Mensch das Recht, über die Erhebung und Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen. Dieses Recht darf nach Art. 4 a Abs. 2 LV nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern. Das verfassungsrechtliche Gebot des Schutzes der personenbezogenen Daten richtet sich dabei nicht nur an die Exekutive, sondern auch an das Parlament.

Bei der Veröffentlichung von Antworten der Landesregierung auf parlamentarische Anfragen durch die Landtagsverwaltung sind zunächst die den jeweiligen Verfassungsorganen zugewiesenen Aufgaben voneinander abzugrenzen: Nach Art. 89 a Abs. 1 LV obliegt es der Landesregierung, parlamentarische Anfragen zu beantworten. Spiegelbildlich dazu stehen dem einzelnen Abgeordneten bzw. einer Fraktion als Ausfluss des parlamentarischen Kontrollauftrages gegenüber der Landesregierung der verfassungsrechtliche Anspruch auf umfassende und fristgerechte Beantwortung ihrer Anfrage zu. Dieser Anspruch ist mit der Zuleitung der Antwort an den bzw. die Fragesteller erfüllt.

Die Veröffentlichung der parlamentarischen Anfragen und der Antworten der Landesregierung ist in den §§ 92 Abs. 5, 97 Abs. 3 i. V. m. 67 Abs. 1 GOLT geregelt und als eigenständige, nicht zur inhaltlichen Beantwortung der Anfrage akzessorische Aufgabe dem Parlament zugewiesen. Dies folgt aus dem allgemeinen Kontrollauftrag des Landtags, der einerseits durch die innerparlamentarische Unterrichtung sämtlicher Abgeordneter mit der Möglichkeit einer daraus resultierenden parlamentarischen Erörterung (vgl. § 93 Abs. 1 und 2 GOLT), daneben aber auch durch eine außerparlamentarische Veröffentlichung als Landtagsdrucksache und der sich daraus ergebenden allgemeinen Publizitätswirkung wahrgenommen wird.

Im Hinblick auf die Beachtung des in Art. 4 a Abs. 1 LV enthaltenen Grundrechtes auf informationelle Selbstbestimmung bedeutet dies, dass jeder Beteiligte (Landesregierung und Landtag) für den Schutz des informationellen Selbstbestimmungsrechtes in seinem Aufgaben- und Tätigkeitsbereich verantwortlich ist. Demnach haben die Landesregierung den Inhalt der Antwort auf eine parlamentarische Anfrage und der Landtag bzw. die Landtagsverwaltung den Inhalt der Veröffentlichungen auf deren datenschutzrechtliche Zulässigkeit zu überprüfen. Folgerichtig hat die Landesregierung nach Art. 89 a Abs. 3 LV und § 91 Abs. 2 GOLT u. a. das Recht, die Beantwortung von parlamentarischen Anfragen abzulehnen, wenn dem Bekanntwerden des Inhalts schutzwürdige Interessen einzelner entgegenstehen. Gleiches gilt auch für den Landtag bei der Wahrnehmung der dem Parlament zugewiesenen

Veröffentlichungsaufgabe: Nach § 5 Abs. 1 DSO-LT dürfen personenbezogene Daten in Landtagsdrucksachen nur dann veröffentlicht werden, wenn dies zur Erfüllung parlamentarischer Aufgaben erforderlich ist und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Daraus folgt, dass die Landtagsverwaltung als für die Veröffentlichung zuständige Stelle in jedem Einzelfall auch zu prüfen hat, ob die Veröffentlichung von Antworten der Landesregierung auf parlamentarische Anfragen auch personenbezogene Daten betrifft und ob der Veröffentlichung, obwohl sie in Erfüllung einer parlamentarischen Aufgabe erfolgt, nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Verfassungsrechtliche Bedenken gegen diese aufgabenspezifische Zuordnung der datenschutzrechtlichen Prüfungsbefugnis bestehen nicht. Ausgehend von der bereits verfassungsrechtlich angelegten Aufgabentrennung zwischen der Landesregierung hinsichtlich der dieser zustehenden inhaltlichen Beantwortung parlamentarischer Anfragen und dem Landtag hinsichtlich der diesem obliegenden über den Beantwortungsanspruch des Fragestellers hinausgehenden Veröffentlichung ist die auch datenschutzrechtlich getrennte Verantwortlichkeit bzw. die daraus resultierende Prüfungsbefugnis nur folgerichtig. Insbesondere der verfassungsrechtlich garantierte Beantwortungsanspruch des Fragestellers wird dadurch nicht verletzt, da unabhängig von der datenschutzrechtlichen Prüfungsbefugnis des Landtags die Antwort der Landesregierung in der vorliegenden Fassung dem Fragesteller zugeleitet wird.

23.2 Weitergabe von Wasserverbrauchszahlen an Entsorgungsbetriebe

Ein Wasserwerk-Zweckverband fragte an, ob er die von ihm abgelesenen Wasserverbrauchszahlen mit den Namen der Betroffenen an die für das jeweilige Gebiet zuständigen Entsorgungsbetriebe übermitteln durfte. Diese nutzten die Verbrauchszahlen, um daraus die Abwassergebühren zu berechnen.

Wenn eine solche Datenübermittlung nicht im Vertrag mit den Verbrauchern oder in einer Satzung geregelt ist, richtet sich die Zulässigkeit nach allgemeinen datenschutzrechtlichen Bestimmungen. Da es sich beim Zweckverband um einen Eigenbetrieb handelte, war das LDSG anwendbar. Danach ist eine Datenübermittlung an andere öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der empfangenden Stelle liegenden Aufgabe erforderlich ist und eine Datenerhebung bei Dritten zulässig wäre. Die übermittelten Verbrauchsdaten waren für die empfangenden Entsorgungsbetriebe erforderlich, um die Abwassergebühren zu errechnen. Hätte eine Übermittlung nicht stattgefunden, hätten die Entsorgungsbetriebe die Verbrauchswerte nur dann erhalten können, wenn sie ebenfalls die Zähler bei den Betroffenen abgelesen hätten. Dies bedeutete für die Verbraucher einen erhöhten Aufwand, da sie zweimal das Ablesen hätten ermöglichen müssen. Es war daher offensichtlich, dass die Datenübermittlung im Interesse der Betroffenen lag und kein Grund zur Annahme bestand, dass sie in Kenntnis des Zwecks ihre Einwilligung verweigern würden. Zudem hätte das Ablesen durch die jeweiligen Entsorgungsbetriebe einen unverhältnismäßigen Aufwand im Sinne des LDSG bedeutet. Die Übermittlung der Verbrauchsdaten an die Entsorgungsbetriebe war daher als zulässig zu bewerten.

23.3 Datenweitergabe durch die Bauämter an die Bekämpfungsstelle „BillB“ der zuständigen Arbeitsämter

Ein Arbeitsamt hatte angeregt, dass die zuständigen Bauämter der Kommunalverwaltungen die Bekämpfungsstelle „BillB“ über Bauprojekte größeren Umfangs informieren sollten, um die Schwarzarbeit besser bekämpfen zu können. Dabei sollten auch personenbezogene Daten der Bauherren übermittelt werden. Hiergegen äußerte eine Kreisverwaltung datenschutzrechtliche Bedenken – zu Recht:

Die Zusammenarbeit zwischen den Arbeitsämtern und den nach dem SchwarzArbG zuständigen Behörden, also den Kreis- und Stadtverwaltungen, ist sowohl im SchwarzArbG als auch im SGB III geregelt. Nach § 3 Abs. 1 SchwarzArbG arbeiten die Kreis- bzw. Stadtverwaltungen als zuständige Behörden mit den Arbeitsämtern zusammen. Eine Datenübermittlung in Fällen der Zusammenarbeit ist auf Einzelfälle beschränkt, in denen sich konkrete Anhaltspunkte für Verstöße gegen bestimmte Gesetze ergeben. Die hier fragliche Datenübermittlung sollte sich aber nicht auf konkrete Verdachtsfälle beschränken, sondern auch solche Bauvorhaben erfassen, bei denen bisher noch keinerlei Anhaltspunkte für einen Gesetzesverstoß vorlagen. Eine Datenübermittlung aufgrund des SchwarzArbG war daher nicht zulässig.

Eine weitere Datenübermittlungsgrundlage ist § 308 Abs. 1 SGB III zu entnehmen. Danach sind die Kreis- bzw. Stadtverwaltungen als zuständige Behörden nach dem SchwarzArbG berechtigt, die für die Prüfungen des Arbeitsamtes erforderlichen Daten einschließlich personenbezogener Daten zu übermitteln. Fraglich war, inwieweit eine generelle Übermittlung personenbezogener Daten von Bauherren an die Arbeitsämter als erforderlich angesehen werden konnte. Ging man davon aus, dass die Arbeitsämter auch ohne konkrete Anhaltspunkte Bauvorhaben stichprobenartig überprüften, war es aus Sicht des LfD ausreichend, wenn die Kreisverwaltungen auf Bauvorhaben hinwiesen, ohne hierbei personenbezogene Daten zu übermitteln. Stellte sich aufgrund der Überprüfung heraus, dass der Verdacht eines Gesetzesverstoßes bestand, konnten in diesen Fällen personenbezogene Daten an die Arbeitsämter übermittelt werden. Eine generelle Übermittlung solcher Daten ohne konkrete Anhaltspunkte für einen Gesetzesverstoß war auch auf der Grundlage von § 308 SGB III unzulässig.

23.4 Recht der Presse auf Akteneinsicht oder Auskunft

Eine Kreisverwaltung wollte wissen, ob sie der Presse Einsicht in oder Auskunft aus Bauakten gewähren durfte bzw. musste. Ein solches Recht der Presse war zu verneinen. Nach dem Landespressegesetz sind die Behörden zwar verpflichtet, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Die Auskünfte können jedoch verweigert werden, wenn ein schutzwürdiges privates Interesse verletzt würde. Die Behörde hat also nach pflichtgemäßem Ermessen zu prüfen, ob eine solche Verletzung durch Informationsweitergabe eintreten würde. Dem Informationsrecht der Presse steht der Anspruch der Beteiligten an einem Verwaltungsverfahren auf Geheimhaltung gem. § 30 VwVfG gegenüber. Danach hat der Beteiligte Anspruch darauf, dass seine Geheimnisse von der Behörde nicht unbefugt offenbart werden. Geheimnisse sind alle Angaben, die der Betroffene in einem Verwaltungsverfahren im Vertrauen auf die Verschwiegenheit der Verwaltung gemacht hat. Darunter fallen auch die Inhalte einer Bauakte. Folglich konkretisiert sich das der Behörde nach Landespressegesetz eingeräumte Ermessen durch den Anspruch auf Geheimhaltung gem. § 30 VwVfG zu einer Verpflichtung der Behörde, die Auskunft zu verweigern.

23.5 Einsicht durch Architekten in Bauakten

Der LfD wurde darauf aufmerksam, dass man unter Architekten die Frage diskutierte, in welchem Umfang diese Einsicht in Bauakten nehmen dürften. Er hat daraufhin die Architektenkammer auf folgende datenschutzrechtliche Gesichtspunkte aufmerksam gemacht und gebeten, diese Bewertungsmaßstäbe den Mitgliedern bei Bedarf zugänglich zu machen:

Regelungen zu personenbezogenen Daten in Bauverfahren finden sich in § 14 BauuntPrüfVO. Dort werden die Voraussetzungen der Übermittlung personenbezogener Daten an andere Behörden und private Stellen genannt. Das Recht auf Einsicht in Bauakten richtet sich nach den Vorschriften des Verwaltungsverfahrensgesetzes bzw. nach dem LDSG. Evtl. kommt auch ein Recht auf Auskunft nach dem Umweltinformationsgesetz in Betracht (vgl. 17. Tb., Tz. 23.2). Eine Einsichtnahme durch Architekten in Bauakten setzt also voraus, dass deren rechtliche Interessen durch das Verfahren berührt werden. Dies hat der betroffene Architekt entsprechend glaubhaft vorzutragen. Die Behörde entscheidet sodann nach pflichtgemäßem Ermessen, ob und in welchem Umfang sie Akteneinsicht gewährt. Wenn der Architekt im Auftrag tätig wird, müssen die genannten Voraussetzungen für den Auftraggeber vorliegen. Der Architekt hat entsprechend nachzuweisen, dass er im Auftrag eines Dritten handelt. Ergibt sich dies nicht aus anderen dem Bauamt bereits vorliegenden Unterlagen, ist der Nachweis in der Regel durch eine schriftliche Vollmacht zu führen.

Folglich besteht kein generelles Einsichtsrecht von Architekten in Bauunterlagen.

23.6 Informationsreise der Kommission beim LfD nach Wien

Die Kommission beim LfD unter Leitung ihres Vorsitzenden, Herrn Abgeordneten Franz Josef Bischel, reiste im Juni 2003 nach Wien, um sich dort über die Umsetzung der europäischen Datenschutzrichtlinie zu informieren. Die Reise wurde von der Geschäftsstelle des LfD vorbereitet und vom Landesbeauftragten begleitet. Die Teilnehmer tauschten Informationen mit Mitgliedern der Österreichischen Datenschutzkommission, des Österreichischen Datenschutzrates sowie mit dem Präsidialchef des Bundeskanzleramtes aus.

24. Schlussbemerkung

24.1 Zur Situation der Geschäftsstelle

Im Bereich des technisch-organisatorischen Datenschutzes konnten die Personalkapazitäten von 1,5 Stellen auf 2,5 Stellen ausgeweitet werden. Für diese Verbesserung der Stellensituation dankt der LfD dem Landtag ausdrücklich. Nachdem es auch gelungen ist, die neue Stelle mit einem sehr qualifizierten Mitarbeiter zu besetzen, wird es möglich sein, die Beratungs- und Kontrolltätigkeit in diesem Bereich ein erhebliches Stück weiter an den tatsächlichen Bedarf anzunähern.

Durch den länger dauernden Ausfall einer Referentin waren deren Aufgaben im Rahmen der bestehenden Vertretungsregelung wahrzunehmen. Dies führt zwangsläufig zu einer erheblichen Einbuße im Hinblick auf die Prüfungsdichte und die Zahl der Beratungen; auf Dauer würde dies zu einer empfindlichen Beeinträchtigung der Aufgabenwahrnehmung des LfD führen. Der LfD wird sich ggf. um einen personellen Ausgleich bemühen.

Die wirtschaftliche Situation des Landes mit der daraus folgenden Haushaltssperre hat unmittelbare Auswirkungen auf die Tätigkeit des LfD. Er verschließt sich selbstverständlich diesen Notwendigkeiten nicht; wichtig ist aber, dass daraus keine völlige Einstellung oder auch nur erhebliche Beschränkung seiner Kontrolltätigkeiten, die zwangsläufig jeweils mit Ausgaben (Reisekosten, Aufwand für externe Unterstützung bei der Prüfung von EDV-Systemen) verbunden sind, folgen darf. Auch zwangsläufige Ersatzbeschaffungen der EDV-Ausstattung der Dienststelle können nicht aufgeschoben werden. Der LfD hat stets ausgesprochen sparsam gewirtschaftet und seine Haushaltsansätze insgesamt nie völlig ausgeschöpft. Der Steuerbürger kann sich darauf verlassen, dass der LfD sich bei seinen Ausgaben auf das Nötigste beschränkt.

24.2 Zusammenarbeit mit anderen Datenschutzinstitutionen

Wie in der Vergangenheit hat der LfD auch im Berichtszeitraum intensiv mit den Datenschutzbeauftragten der anderen Länder und dem des Bundes eng zusammengearbeitet. Die Tätigkeit der zu diesem Zweck eingerichteten Arbeitskreise und der beiden jährlichen Gesamtkonferenzen findet einen wesentlichen Niederschlag in den verabschiedeten Entschließungen, Beschlüssen und Arbeitspapieren. Diese sind nahezu vollständig in den Anlagen zu diesem Bericht abgedruckt. Turnusgemäß hat der LfD die Gesamtkonferenzen des Jahres 2002 als Gastgeber ausgerichtet und geleitet. Die Frühjahrskonferenz fand in Mainz, die Herbstkonferenz in Trier statt. Besonderer Dank gilt dem Herrn Ministerpräsidenten für einen Empfang, den er der Konferenz gab, sowie dem Herrn Präsidenten des Landtags für einen Empfang in Trier.

Nicht selten waren Beschwerdeführer zuständigkeitshalber an die Datenschutzaufsichtsbehörde für den privaten Bereich, die Aufsichts- und Dienstleistungsdirektion (ADD) in Trier, zu verweisen. Es gab auch vereinzelt DV-Projekte wie z. B. die Patientenchipkarte im Bereich der KV Trier, an denen die ADD in ihrer Eigenschaft als Datenschutzaufsichtsbehörde neben dem LfD beteiligt war. In allen Fällen hat sich deren Arbeit als engagiert und den Datenschutz fördernd erwiesen; davon legt auch ihr jüngst erschienener Tätigkeitsbericht Zeugnis ab (Erster Tätigkeitsbericht der ADD als Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich in Rheinland Pfalz für den Zeitraum vom 1. Juni 2001 bis zum 31. Mai 2003, im Internet unter www.add.rlp.de abrufbar).

Auch die besonders engen Kontakte zum hessischen Datenschutzbeauftragten wurden gepflegt und vertieft.

Das virtuelle Datenschutzbüro, der gemeinsame Internetauftritt der Datenschutzbeauftragten aus Deutschland, der Schweiz, den Niederlanden und Kanada, hat sein Angebot erweitert und verbessert. Es ist unter „www.datenschutz.de“ abrufbar und genießt inzwischen weite Akzeptanz.

Im Berichtszeitraum hat wiederum ein Meinungsaustausch mit dem Datenschutzbeauftragten des ZDF (Herrn Christoph Bach) und des Südwestrundfunks (Herrn Prof. Dr. Armin Herb) stattgefunden. Die Erörterung von Fragen gemeinsamen Interesses hat erneut eine erfreuliche inhaltliche Übereinstimmung ergeben.

Die Kommission beim LfD hat ihre gesetzliche Aufgabe, den LfD bei der Wahrnehmung seiner Aufgaben zu unterstützen und den Tätigkeitsbericht vorzuberaten, wiederum engagiert wahrgenommen. Im Berichtszeitraum ist Herr Abg. Johannes Berg verstorben. An seine Stelle ist Herr Abg. Baldauf getreten. Außerdem hat Herr Abg. Dr. Schiffmann die Stelle des nunmehr als Landrat tätigen Abg. Axel Redmer übernommen. Herr Abg. Bischel hat weiterhin den Vorsitz mit großer fachlicher Kompetenz und parteiübergreifender gelassener Souveränität geführt. Auch allen anderen Mitgliedern, wozu außer den Vorgenannten die Abg. Frau Reich, Herr Pörksen, Herr Dr. Peter Schmitz, Herr Wiechmann und Herr Staatssekretär Bruch gehören, gilt der persönliche Dank des LfD für die vertrauensvolle Zusammenarbeit.

Der Verwaltung des Landtags, insbesondere dem Präsidenten, dem neu berufenen Direktor Professor Dr. Klaus-Eckart Gebauer sowie insbesondere der Personalabteilung, der Druckerei und der Poststelle gilt der besondere Dank für die Unterstützung bei der Wahrnehmung der Verwaltungsaufgaben des LfD. Den Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle gebührt Dank und Anerkennung für ihren engagierten, kompetenten und umsichtigen Einsatz bei der Erfüllung ihrer häufig recht schwierigen Aufgaben.

24.3 Internetangebot des LfD

Bereits seit mehreren Jahren ist der LfD unter www.datenschutz.rlp auch im Internet vertreten; das Internetangebot pflegt der LfD selbst. Neben zahlreichen Materialien zum Datenschutz, u. a. Hinweise, Empfehlungen und Orientierungshilfen zu speziellen Themen, sind auch die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebenen Entschließungen enthalten. Fernerhin sind seit 1981 alle Tätigkeitsberichte des LfD gegliedert nach Sachgebieten abrufbar.

Der LfD hofft – vor dem Hintergrund seiner begrenzten personellen Ausstattung – dem steigenden Beratungsbedarf der Verwaltungen in stärkerem Maße auch mit dem Internet-Angebot Rechnung tragen zu können. Fernerhin möchte der LfD damit den neu bestellten behördlichen Datenschutzbeauftragten den Einstieg in das komplexe Thema „Datenschutz“ erleichtern und allen anderen Interessierten die Möglichkeit geben, sich über spezielle datenschutzrechtliche Themen und deren Beurteilung durch den LfD zu informieren.

Im Berichtszeitraum erfolgten auf die Internetseiten des LfD jährlich ca. 200 000 Zugriffe. Diese Zahl zeigt das starke Interesse und belegt, dass sich die Mühe für die Pflege und den Ausbau des Internetangebotes lohnt.

24.4 Resümee und Ausblick

Als Fazit der vergangenen beiden Jahre bleibt festzuhalten:

Das informationelle Selbstbestimmungsrecht steht zunehmend unter Druck.
Nicht nur staatliche Handlungen, auch und gerade Aktivitäten der Wirtschaft sind hier zu nennen:
Marketingfirmen können das Handy und seine Standortinformationen zu Werbezwecken nutzen (unter Ausnutzung der „location based services"); Datamining und Data-Warehouses und damit verbundenen Scoring-Verfahren der verschiedensten Art bleiben bedeutsam. Das Scoring-Verfahren der Schufa beispielsweise begründet eine unangemessene Objektstellung des Betroffenen: Er erhält keine Auskunft über seinen Scorewert, ebenso wenig über die Kriterien, die diesen Wert begründen (vgl. Möller/Florax, NJW 2003, S. 2724).

Kleine, meist unsichtbare Sender können überall, z. B. in der Kleidung oder in Verpackungen, eingebaut werden, um Daten zu liefern („Pervasive computing"). Dazu gehören auch die sog. „Smart Chips" oder „RFID-Chips" (Radio Frequency Identification), die – klein wie ein Stecknadelkopf – in jedes Produkt eingebracht werden können (vgl. Entschließung der internationalen Konferenz der Datenschutzbeauftragten in Sydney, im Internet abrufbar unter http://privacyconference2003.org).

Neue Gefahren entstehen durch Foto-Handys: Sie sind nicht nur zur Industrie-Spionage geeignet, sondern sie begründen eine tiefgreifende Gefährdung des Rechts am eigenen Bild (s. FAZ vom 12. Juli 2003, S. 17).

Bei der Nutzung des Internets denken Surfer häufig nicht daran, dass ihre Aktivitäten im Netz dokumentiert werden. Sie wissen oft nicht, dass Web-Bugs oder Cookies, die auf der Festplatte lagern, möglicherweise an andere Web-Server Daten liefern oder ihr Surfverhalten in Protokolldateien festgehalten wird. Die Preisgabe des Namens in einem Formular kann die entscheidende Aktion sein, um zu ermöglichen, dass die in Cookies gespeicherten oder von Web-Bugs gesammelten Daten zu einem Persönlichkeitsprofil personenbezogen zusammengefasst werden.

Im staatlichen Bereich seien ebenfalls kurz die spektakulärsten Entwicklungen genannt:

Auf europäischer Ebene wachsen zentrale Institutionen und Datenbanken, die Verdächtigendaten speichern: Das Schengener Informationssystem, EUROPOL, EUROJUST und die Bemühungen zur Schaffung einer europäischen Staatsanwaltschaft sind zu nennen.

Die EU formuliert Anforderungen an die Telekommunikationsinfrastruktur, um die Überwachung der Telekommunikation für die Sicherheitsdienste zu erleichtern (Enfopol 98; vgl. dazu 17 Tb., Tz. 3.7, Anforderung der „Data Retention"; Entschließung der europäischen Konferenz der DSBen in Cardiff vom 9. September 2002, vgl. Anlage 35).

Die Aufnahme von biometrischen Daten in Ausweispapieren ist beschlossen: Dies gehört zum Arbeitsprogramm der OECD, Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre (– WPISP –; S. 79 des 10. Tätigkeitsberichts 2002/2003 des Eidgenössischen Datenschutzbeauftragten).

Die Genanalyse im Strafverfahren wird ausgeweitet.

Die Polizeigesetze der Länder (auch das rheinland-pfälzische, s. Tz. 5.1) erhalten katalogartige weitreichende Befugnisse zur heimlichen Informationsgewinnung (z. B. Telefonüberwachungsmaßnahmen, Video-Überwachung, Großer Lausch- und Spähangriff).

Verfahren zum „E-Government" setzen auf Effizienz und Schnelligkeit, gelegentlich unter Vernachlässigung des Datenschutzes. In diesem Bereich ist besonders bedauerlich, dass ein schrankenloses Direktzugriffsverfahren auf das automatisierte Grundbuch unter Vernachlässigung datenschutzrechtlicher Standards eingerichtet wird.

Die zunehmende Verlagerung staatlicher Datenverarbeitungsaufgaben auf private Auftragnehmer muss aus Datenschutzsicht weiterhin kritisch beobachtet werden. Mittelfristig erweist sich häufig, dass ein Verlust an Einwirkungsmöglichkeiten, wettbewerbsbedingte Veränderungen bei den Auftragnehmern, Intransparenzen und Abhängigkeiten Rationalisierungseffekte relativieren. Zentrales Augenmerk ist darauf zu richten, dass die Kontroll- und Steuerungsmöglichkeiten der Verwaltung erhalten bleiben und Outsourcing nicht zu einer Absenkung des Datenschutzniveaus führt.

Man kann darüber streiten, ob die wirtschaftliche und finanzielle Lage und damit die Sparnotwendigkeiten der öffentlichen Hand den größten Druck aufbauen oder ob vielmehr die Bedrohungslage durch internationalen Terrorismus und organisierte Kriminalität sowie die dadurch hervorgerufenen staatlichen Maßnahmen im Vordergrund der Besorgnisse der Datenschützer stehen müssen. Zum Teil sind beide Gesichtspunkte auch miteinander verwoben: Die verschlechterte globale Wirtschaftslage ist sicher ein bedeutsamer Hintergrund für wachsende Kriminalität und für die Ausweitung extremistischer und terroristischer Tätigkeiten.

Diese Gesamtlage jedenfalls führt dazu, dass das Gewicht der Argumente, die für den Datenschutz und damit für die individuellen Freiheiten der Bürger sprechen, zurückgedrängt werden durch Gesichtspunkte der Allgemeininteressen, der allgemeinen Sicherheit, der Erhöhung der Verteilungsgerechtigkeit bei staatlichen Leistungen sowie der Maßnahmen, die für die wirtschaftliche Entwicklung Impulse setzen. Abwehrschlachten des Datenschutzes in diesem Bereich sind selten erfolgreich. Der Entwurf des rheinland-pfälzischen Polizeigesetzes ist nur ein Beispiel dafür. Die Reform des Gesundheitswesens und der sozialen Sicherungssysteme wird sicherlich ebenfalls mit einer Einschränkung von Patientenrechten bzw. einer Erweiterung der Datenzugriffsmöglichkeiten für solche Institutionen einhergehen, die Kosten zu kontrollieren haben.

Schließlich nehmen die Aktivitäten der Wirtschaft zu, um das Konsumentenverhalten möglichst genau erkennen und Angebote möglichst zielgerichtet formulieren zu können. Dem dienen die meisten oben genannten neuen technischen Entwicklungen im Bereich der Privatwirtschaft.

Auch vor diesem Hintergrund aber muss der Datenschutzbeauftragte die Bedeutung des Grundrechts auf Datenschutz betonen, selbst wenn die Chance darauf geringer wird, dass in allen Bereichen ein wirklich tragfähiger Kompromiss erzielt wird. Der Datenschutzbeauftragte muss sich darum bemühen, das Grundrecht zur Geltung zu bringen.

Legitim und wichtig ist andererseits aber auch, dass der Datenschutzbeauftragte an der technischen Gestaltung im Sinne von Datenvermeidung und Datensparsamkeit, also der Begrenzung auf das wirklich Erforderliche, mitwirkt. Gerade im Bereich des E-Government, das nicht nur unter Einsparungsgesichtspunkten immer größere Bedeutung gewinnt, muss er darauf hinwirken, datenschutzgerechte Lösungen zu finden.

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz hat nie zu den Pessimisten im Kreis der Datenschützer gezählt; im Gegenteil, er hat in all den Jahren seiner Tätigkeit immer wieder betont, dass die technische Entwicklung durchaus Anlass zu einer optimistischen Grundhaltung auch unter dem Aspekt des informationellen Selbstbestimmungsrechtes gibt. Insgesamt muss aber konstatiert werden, dass die letzten beiden Jahre in einigen Punkten den Skeptikern in diesem Bereich Recht gegeben haben. Es bleibt zu hoffen, dass die eingangs erwähnten globalen Entwicklungen der Wirtschaft und der Kriminalität nicht dauerhaft das Klima bestimmen. Gerade unter diesen Bedingungen aber wird der LfD seine Funktion als Mahner und Wächter eines bedeutsamen modernen Grundrechts weiterhin engagiert wahrnehmen.

Anlage 1

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 2

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

– Informationsaustausch mit Partnern

  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

– Verarbeitung personenbezogener Daten

  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

– Ermittlungsindex und Dateien

  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

– Auskunftsrecht

  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

– Änderung, Berichtigung und Löschung

  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

– Speicherungsfristen

Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z. B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

– Datensicherheit

Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

– Gemeinsame Kontrollinstanz

Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindenden Charakter haben.

– Rechtsschutz

Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

– Rechtsetzungsbedarf

Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 3

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
Lkw-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechnungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

– Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
– Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
– Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
– Es ist sicherzustellen, dass anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

Anlage 4

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (Grundsatz der Freiwilligkeit).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,
– ob ihre Daten auf einer Chipkarte gespeichert werden,
– welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
– welche ihrer Daten auf der Karte wieder gelöscht werden,
– ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
– welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der Krankenversichertenkarte gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offen legen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z. B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 5

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
„Neue Medienordnung“

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anlage 6

Entschließung
der 62. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. bis 26. Oktober 2001
Gesetzliche Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegenzunehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage
zur Entschließung „Gesetzliche Regelung von genetischen Untersuchungen“
Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

Zu regeln ist die Zulässigkeit genetischer Untersuchungen beim Menschen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten. Neben allgemeinen Regelungen sind besondere Bestimmungen zu genetischen Untersuchungen
1. zu medizinischen Zwecken
2. im Zusammenhang mit Arbeits- und Versicherungsverhältnissen
3. zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung
4. zu Forschungszwecken

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.

(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. Genetische Untersuchungen: Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS/RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;
2. Prädiktive Untersuchungen: vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;
3. Überträgerstatus: Erbablagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden;
4. Pränatale Untersuchungen: vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;
5. Reihenuntersuchung: genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;
6. Diagnostische genetische Untersuchungen: genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;
7. Probe: die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;
8. Genetische Daten: im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;
9. Betroffene Person: die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau;
10. Verarbeiten: das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

Genetische Untersuchungen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten bedürfen der freiwilligen, schriftlichen Einwilligung der betroffenen Person nach Aufklärung. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen zu regelnden und in der Strafprozessordnung geregelten Ausnahmen.

Zulassung zur Durchführung genetischer Untersuchungen

(1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung durch die zuständige Aufsichtsbehörde des Landes.

(2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass
- die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,
- die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und
- in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.

(3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

Genetische Testverfahren dürfen nur für den Gebrauch durch Ärztinnen, Ärzte oder Labors eingeführt oder in Verkehr gebracht werden. Das öffentliche Angebot, genetische Untersuchungen zu medizinischen Zwecken ohne individuelle Beratung der betroffenen Person durchzuführen, ist unzulässig. Die Berufsfreiheit, Artikel 12 Absatz 1 Satz 2 Grundgesetz, wird insoweit eingeschränkt.

Zweckbindung

Die für die genetische Untersuchung vorgesehene oder genutzte Probe und die genetischen Daten dürfen nur für den Zweck verwandt und für die Dauer aufbewahrt werden, zu denen die betroffene Person ihre Einwilligung erklärt hat oder zu denen ein Gericht oder eine Verwaltungsbehörde eine Anordnung getroffen hat. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen geregelten Ausnahmen.

Datensicherheit

(1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und datenverarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.

(2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.

(3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundesdatenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

Die betroffene Person hat das Recht, unentgeltlich Einsicht in die Dokumentationen zur genetischen Untersuchung einschließlich Aufklärung und Beratung zu nehmen und Auskunft über die zu ihr gespeicherten Daten zu verlangen.

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

(1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.

(2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.

(3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Für darüber hinausgehende genetische Untersuchungen gelten die Richtlinien der Bundesärztekammer zur pränatalen Diagnostik. Das Geschlecht darf gezielt nur zu medizinischen Zwecken festgestellt werden. Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DNA-Untersuchungen sein dürfen, muss der gesellschaftspolitischen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben.

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

(1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.

(2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

(1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.

(2) Voraussetzung für die Zulassung ist, dass
- die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,
- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

(1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.

(2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

(1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.

(2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über
- Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung,
- mögliche, auch unerwartete Ergebnisse der Untersuchung,
- mögliche Folgen des Untersuchungsergebnisses, einschließlich physischer und psychischer Belastungen der betroffenen Person oder ihrer Familie,
- Behandlungsmöglichkeiten für die gesuchte Krankheit,
- den geplanten Umgang mit der Probe und den genetischen Daten einschließlich des Orts und der Dauer der Aufbewahrung bzw. Speicherung,
- die Einflussmöglichkeiten und Datenschutzrechte der betroffenen Person,
- weitere Beratungs- und Unterstützungsmöglichkeiten.

(3) Aufklärung und Beratung dürfen nur der individuellen und familiären Situation der betroffenen Person und den möglichen psychosozialen Auswirkungen des Untersuchungsergebnisses auf sie und ihre Familie Rechnung tragen.

(4) Bei Reihenuntersuchungen kann in begründeten Ausnahmefällen die Aufklärung in standardisierter Form erfolgen, wenn zugleich die Möglichkeit einer zusätzlichen individuellen Beratung angeboten wird.

(5) Bei pränatalen Untersuchungen ist der Partner der betroffenen Frau in die Beratung einzubeziehen, sofern die Frau einwilligt. Auf Stellen der Schwangerschaftskonfliktberatung ist hinzuweisen.

(6) Bei genetischen Untersuchungen zum Erkennen eines Überträgerstatus soll der Partner oder die Partnerin der betroffenen Person in die Aufklärung und Beratung einbezogen werden.

Einwilligung

(1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,
– ob die genetische Untersuchung durchgeführt werden soll,
– welches Ziel die genetische Untersuchung hat,
– ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,
– wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.
Soweit die betroffene Person vom Ergebnis, auf das die Untersuchung zielt, keine Kenntnis nehmen will, soll außer bei Reihenuntersuchungen grundsätzlich auf die genetische Untersuchung verzichtet werden.

(2) Die betroffene Person oder ihr gesetzlicher Vertreter hat die vorherige Aufklärung und Beratung schriftlich zu bestätigen und die Einwilligung in die genetische Untersuchung und in den vereinbarten Umgang mit der Probe und den genetischen Daten schriftlich zu erklären.

(3) Die Einwilligung kann widerrufen werden mit der Folge, dass noch nicht erfolgte Maßnahmen unterbleiben, schon vorliegende Proben vernichtet und die im Zusammenhang mit der Untersuchung erhobenen und gespeicherten Daten gelöscht werden.

Unterrichtung über das Untersuchungsergebnis

(1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.

(2) Ist das Ergebnis nach ärztlicher Erkenntnis auch für Verwandte der betroffenen Person von Bedeutung, hat die Ärztin oder der Arzt bei der nachgehenden Beratung der betroffenen Person auch auf das Recht der Verwandten hinzuweisen, ihre Erbanlagen nicht zur Kenntnis zu nehmen. Will die betroffene Person die Verwandten gleichwohl unterrichten, soll die Beratung auch die Möglichkeit umfassen, die Ärztin oder den Arzt mit der Unterrichtung von Verwandten der betroffenen Person zu beauftragen.

(3) Gegen den Willen der betroffenen Person oder ihres gesetzlichen Vertreters darf die veranlassende Ärztin oder der veranlassende Arzt Verwandte oder Partner der betroffenen Person nur dann von dem Untersuchungsergebnis unterrichten, wenn und soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Diagnostische genetische Untersuchung bei behinderten Personen

Bei diagnostischen genetischen Untersuchungen, die sich auf die Ursache einer Behinderung der betreffenden Person beziehen, gelten die Anforderungen an die Einwilligung und Unterrichtung über das Untersuchungsergebnis entsprechend.

Genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

Grundsatz

Arbeitgebern und Versicherern ist es verboten, als Voraussetzung für einen Vertragsabschluss oder während des Vertragsverhältnisses prädiktive genetische Untersuchungen an betroffenen Arbeits- oder Versicherungsvertragsbewerbern oder Vertragspartnern durchzuführen oder zu veranlassen oder Ergebnisse von genetischen Untersuchungen zu verlangen, entgegenzunehmen oder sonst zu nutzen. Aus einer wahrheitswidrigen Beantwortung können Arbeitgeber oder Versicherer grundsätzlich keine Rechte ableiten (Ausnahmen siehe unten).

Arbeitsverhältnis

Bleibt der Arbeitsplatz trotz vorrangiger Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr verbunden, für deren Einritt nach dem Stand der Wissenschaft eine bestimmte Genstruktur der Betroffenen von Bedeutung ist, ist eine Arbeitsplatzbewerberin oder ein Arbeitsplatzbewerber hierauf hinzuweisen. Die Betriebsärztin oder der Betriebsarzt soll die betroffene Person hinsichtlich einer geeigneten genetischen Untersuchung beraten und ihr dafür zugelassene Ärztinnen oder Ärzte benennen.

Ausnahmen für das Versicherungsverhältnis

(1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250 000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.

(2) Bestehen konkrete Anhaltspunkte, insbesondere aufgrund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

(1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.

(2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.

(3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist zehn Jahre aufzubewahren.

Einwilligung

Genetische Untersuchungen zu Zwecken der Abstammungsklärung oder Identifizierung dürfen nur mit schriftlicher Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters oder auf gerichtliche oder behördliche Anordnung durchgeführt werden. Für genetische Untersuchungen zur Abstammungsklärung bei Minderjährigen gilt § 1629 BGB.

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

(1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.

(2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

(1) Für konkrete, zeitlich befristete Forschungsvorhaben ist die genetische Untersuchung von Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten zulässig, wenn

1. die Proben und die genetischen Daten der betroffenen Person nicht mehr zugeordnet werden können oder
2. im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person nach den Anforderungen für Forschungsvorhaben eingewilligt hat (siehe unten) oder
3. im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet noch die Einwilligung eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt und der Forschungszweck nicht auf andere Weise zu erreichen ist.

(2) In den Fällen der Ziffer (1) Nr. 2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.

(3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.

(4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens zehn Jahren zulässig.

(5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer (1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

(1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten). Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.

(2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.

(3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.

(4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicherzustellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.

(5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach fünf Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

(1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über
- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
- das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
- ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,
- die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,
- Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,
- ihr Recht – vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) – die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,
- ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Entpseudonymisierungsverfahrens zu erfahren,
- ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.

(2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.

(3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

(1) Hinsichtlich der genetischen Daten stehen der betroffenen Person die im Bundesdatenschutzgesetz geregelten Rechte zu. Widerruft die betroffene Person ihre Einwilligung (siehe oben), sind entweder die Probe zu vernichten und die genetischen Daten zu löschen oder die Zuordnungsmerkmale zu löschen.

(2) Erbringt ein Forschungsvorhaben Ergebnisse, die für die betroffene Person von Bedeutung sind, veranlasst der Träger des Forschungsvorhabens eine Unterrichtung der betroffenen Person. Dies gilt nicht, wenn die betroffene Person erklärt hat, von dem Untersuchungsergebnis keine Kenntnis nehmen zu wollen (siehe oben).

Treuhänder

(1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.

(2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer
- eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder
- den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben
- oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

(1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit . . . . . bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe . . . . . .

(2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne
- Arzt oder Ärztin zu sein,
- die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,
- die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder
- die Einwilligung der betroffenen Person eingeholt zu haben,

wird mit . . . . . bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit . . . . . bestraft.

(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit . . . . . bestraft.

(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken
- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder
- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit . . . . . bestraft.

Antrag

Die oben aufgeführten Straftaten werden nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und die für die Datenschutzkontrolle zuständige Behörde.

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach In-Kraft-Treten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

Träger von bestehenden Proben- und genetischen Datensammlungen haben der Anzeigepflicht bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung innerhalb von sechs Monaten nach In-Kraft-Treten dieses Gesetzes nachzukommen. Innerhalb dieser Frist ist den Anforderungen an die Einwilligung zu entsprechen. Vor In-Kraft-Treten dieses Gesetzes ohne Einwilligung gewonnene Proben und erhobene genetische Daten sind spätestens nach zwei Jahren zu vernichten bzw. zu löschen. Dies ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen.

Anlage 7

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 7. März bis 8. März 2002
Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 7. März bis 8. März 2002

Positionspapier
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen

1. Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleichlautende Regelungen folgenden Inhalts aufgenommen:

Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
– Fingern,
– Händen oder
– Gesicht
des Inhabers enthalten.

Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
– Arten der biometrischen Merkmale,
– Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
– Art der Speicherung und
– Art ihrer sonstigen Verarbeitung und Nutzung.
Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.

Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2. Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nutzen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild

Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift

Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungsqualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung „Gesicht“ lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, so dass fraglich ist, ob sie durch „Ungeübte“ in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1).

3. Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

- Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
  - Leseeinheit für die aktuellen biometrischen Merkmale,
  - Leseeinheit für die Ausweispapiere,
  - Entschlüsselungs- und Vergleichseinheit und
  - Einheit zur Freigabe bzw. Sperrung der Passage.
- Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.
- Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
- Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
- Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
- Eine regelmäßige Falschrückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
- Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
- Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für den Zeitraum der Gültigkeit der Ausweise).
- Der Schlüssel darf Unbefugten nicht bekannt werden.
- Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

- Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]) herangezogen werden.
- Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acception Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwindungssicherheit ist, umso mehr berechtigte Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.
- Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.
- Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.
- Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1 % bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500 000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4. Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen bzw. mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, – 53 –).

In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5. Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d. h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von „Doppelidentitäten“ durch Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten („Template“, „Vektor“) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6. Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7. Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es, biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zurzeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nicht kooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch – wegen des hierfür erforderlichen Aufwands – nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8. Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlicher Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale bzw. wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft zu werden, als sonst notwendig.

Anlage 8

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 7. März bis 8. März 2002
Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internets kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1. Januar 2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen, z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung, besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 9

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 7. März bis 8. März 2002
zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internets am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internets am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internets am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internets müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Anlage 10

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 7. März bis 8. März 2002
Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 11

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. Mai 2002
Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereitgestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 12

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. und 25. Oktober 2002
zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des World Wide Web), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 13

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. und 25. Oktober 2002
Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zurzeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Anlage 14

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 24. und 25. Oktober 2002
zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anlage 15

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes
  - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
  - Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
  - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
  - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

– Technischer Datenschutz

Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

– Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen. Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

– Förderung von datenschutzgerechter Technik

Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.
Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von allein ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

– Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-Mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internets durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

– Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:
Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internets und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.
Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

Die Evaluierung muss durch unabhängige Stellen und anhand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

– Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die jahrtausendealte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung so weit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten, und zwar auch für deren Verwendung im Einzelfall. Der Bundesgesetzgeber wird auch aufgefordert, gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

– Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen. Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

– Datenschutz im Steuerrecht

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetznovellen und Gesetzentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

– Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

– die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

– die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

– die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

– die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

– Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet. Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

– Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

– Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anlage 16

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,
- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,
- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,
- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,
- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,
- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,
- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und
- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,
- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

Anlage 17

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei E-Commerce und E-Government werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im E-Government detailliert beschreiben können.

Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbaren Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen.[1)]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt.[2)]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

1) Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

2) Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

Anlage 18

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen. So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die
- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

   Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,
   - ob sie überhaupt verwendet wird,
   - welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
   - welche Daten zu löschen sind und wann das zu geschehen hat,
   - ob sie im Einzelfall vorgelegt wird und
   - welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin
- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26. Oktober 2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 3. Mai 2002, wonach „der Patient Herr seiner Daten" sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski", „raucht", „trinkt zwei Biere pro Tag"), diese überwachen und so zur „Gesundheitspolizei" werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

Anlage 19

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

Anlage 20

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. und 28. März 2003
Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3 000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28. Januar 2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen“ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

– Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

– Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.

Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

– Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

– Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

– dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

– den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

– unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

– die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,

– die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

– E-Government- und E-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

– die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

– die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

Anlage 21

Entschließung
der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2003
Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9 802 Anordnungen, waren es im Jahr 2001 bereits 19 896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

Anlage 22

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 2003
Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28. März 2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12. März 2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

Anlage 23

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003
Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

– Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

– Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

– Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die die GEZ künftig auch online zugreifen.

– Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

– Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

Anlage 24

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003
Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

– zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

– zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

Anlage 25

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003
Zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei – oftmals vom Nutzer unbemerkt oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne dass dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.
- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.
- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezoger Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die datenverarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

Anlage 26

Entschließung
der 66. Konferenzder Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. September 2003 in Leipzig
zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.
- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit Data-Warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahin gehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist und dass
- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.
Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

Anlage 27

Entschließung
der 66. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. September 2003 in Leipzig
Konsequenzen aus der Untersuchung des Max-Planck-Instituts
über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai dieses Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Darin hat es festgestellt, dass

– die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2 149; 2001: 3 868) hat,

– die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2 494 um das Sechsfache auf 15 741 gestiegen ist,

– sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3 730 auf 9 122 fast verdreifacht hat,

– in 21 % der Anordnungen zwischen 1 000 und 5 000 Gespräche, in 8 % der Anordnungen mehr als 5 000 Gespräche abgehört worden sind,

– der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

– die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von drei Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu zwei Monaten andauern,

– lediglich 24 % der Beschlüsse substanziell begründet werden,

– es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

– 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen Ultima Ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

– Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

– Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

– Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

– Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100 a StPO muss reduziert werden.

– Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

– Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

– Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

– Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

– Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

– Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anlage 28

66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. September 2003 in Leipzig
Beschluss zu datenschutzrechtlichen Anforderungen an das Projekt „JobCard“

1. Das Grundrecht der informationellen Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Insbesondere darf ein notwendiges Identifikationsmittel nicht die Funktion eines Personenkennzeichens erhalten, mit dem verschiedene Datenbestände geöffnet und zusammengeführt werden können. Für den Bürger muss erkennbar sein, wer wann unter welchen Voraussetzungen auf seine Daten zugreifen kann.

   Deshalb müssen zum einen Verfahren, die es ermöglichen, dass staatliche und private Stellen auf zentrale Speicher mit personenbezogenen Daten zugreifen können, gesetzlich geregelt werden. Zum anderen soll jedoch auch bei einer gesetzlichen Regelung so weit wie möglich der Grundsatz der Freiwilligkeit berücksichtigt werden.

2. Zentraldateien mit umfangreichen Datensammlungen, insbesondere mit sensiblen Daten, begründen erhebliche Gefahren. Sie bedingen die Gefahr der Überwachung und nicht absehbarer Zweckänderungen sowie weiterer Missbrauchsrisiken. Das ist vor allem für zentrale personenbezogene Gesunheitsdateien von größter Bedeutung; diese werden aus Datenschutzsicht als äußerst problematisch angesehen. Für sonstige Zentraldateien ist eine sorgfältige Risiko/Nutzen-Abwägung durchzuführen. Durchgängig ist nach der datenschutzfreundlichsten Lösung zu suchen.

3. Aus dem Volkszählungsurteil folgt, dass nicht jede Stelle, die an dem Projekt beteiligt ist, Zugriff auf den gesamten Datenbestand haben darf. Vielmehr ist hier besonders der Grundsatz der Zweckbindung einzuhalten. Zugriff darf nur durch die zuständigen Stellen auf die dort erforderlichen Daten erfolgen. Dies ist durch technische Maßnahmen sicherzustellen. Insbesondere darf ein für ein Verfahren notwendiges Identifikationsmittel nicht die Funktion eines Pesonenkennzeichens erhalten, mit dem verschiedene Datenbestände geöffnet werden und zusammengeführt werden könnten.

4. Die Arbeitskreise der Datenschutzkonferenz werden gebeten, weiter die Konzeption von Verfahren, die den Zugriff auf personenbezogene Daten mit Hilfe einer Signaturkarte ermöglichen, datenschutzmäßig zu begleiten. Dabei sind insbesondere in sicherheitstechnischer Hinsicht die Konzepte danach zu prüfen, ob zuverlässig die Funktion eines verfassungsrechtlich unzulässigen allumfassenden Personen-Kennzeichens vermieden wird.

Anlage 29

Orientierungshilfe für den Betrieb eines Newsletter-Dienstes

Diese Handreichung soll den Abgeordneten des rheinland-pfälzischen Landtags bei der datenschutzgerechten Gestaltung sog. „Newsletter-Dienste“ als Handlungsempfehlung dienen. Es geht hier um die Möglichkeit, anstelle des herkömmlichen Postversandes die neuen Medien zu nutzen, beispielsweise um die Wahlkreisarbeit darzustellen, um auf Termine für Bürgergespräche hinzuweisen oder über im Parlament gehaltene Reden zu informieren, um Angebote zu Informationsfahrten bis hin zu allgemeiner Wahlwerbung. Der Erfolg eines solchen Dienstes hängt wesentlich vom Vertrauen ab, das ihm seine Nutzer entgegenbringen. Nur dann, wenn ein angemessener Schutz der personenbezogenen Daten gewährleistet ist, werden die Bürgerinnen und Bürger einen solchen Dienst akzeptieren.

Diejenigen, die eine Direktwerbekampagne starten, müssen sich eine große Zahl von E-Mail-Adressen potentieller Interessenten beschaffen. Über das Internet ist dies auf drei Arten möglich: direkte Erfassung der Adressen von Website-Besuchern, Erwerb von Adressenlisten, die von Dritten angeboten werden und Erfassung von Adressen aus öffentlichen Bereichen des Internets wie öffentliche Verzeichnisse oder Newsgroups.

Aus der Sicht der Bürgerinnen und Bürger gibt es ein dreifaches Problem:

Erstens werden E-Mail-Adressen ohne Wissen und Zustimmung erfasst, zweitens erhält man große Mengen unerwünschter Information und drittens werden die Betroffenen mit den Kosten für die Übermittlung belastet, weil ihre Verbindungszeit in Anspruch genommen wird. Bezeichnen könnte man dies als die moderne Variante der Postwurfsendung: Man erhält Werbung bzw. eine Information, ohne dass man sie jemals angefordert hat oder überhaupt haben möchte.

In diesem Zusammenhang tauchen immer wieder zwei neudeutsche Begriffe auf, nämlich das „Opt-in-“ und das „Opt-out-Verfahren“.

Das Opt-in-Verfahren sieht vor, dass der Nutzer ausdrücklich einverstanden sein muss, wenn er Werbemails erhalten möchte. Er kann selbstbestimmt entscheiden, wer seine Mail-Adresse zu welchem Zweck nutzen darf. Hier ist also die Kommunikation vom Nutzer her ausdrücklich erbeten.

Dagegen bedeutet das Opt-out-Verfahren, dass sich der Internetnutzer zur Vermeidung weiterer Werbemails in so genannte „Opt-out-Listen“ austragen muss.

Dahinter stehen zwei bekannte Modelle: Das Opt-out-Verfahren ist vergleichbar mit der Widerspruchslösung, das Opt-in-Verfahren entspricht der Einwilligungslösung.

Was die gegenwärtige Rechtslage anbelangt, so fehlt es hierzu noch an einer expliziten gesetzlichen Regelung. Die Rechtsprechung hat sich zwar schon mehrfach mit unverlangt zugesandten Werbemails befasst und in aller Regel den Schutz der Privatsphäre der Internetnutzer sehr hoch bewertet. Eine Grundsatzentscheidung des BGH ist bislang allerdings noch nicht ergangen.

Diese Rechtslage wird sich jedoch demnächst ändern, und zwar aufgrund einer EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Dort ist in Artikel 13 vorgesehen, dass die Verwendung von elektronischer Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf. Hier wird das „Opt-in-Verfahren“, also das Einwilligungsmodell, festgeschrieben.

Nach der Richtlinie sind Vorkehrungen zu treffen, um die Teilnehmer gegen die Verletzung ihrer Privatsphäre durch unerbetene Nachrichten für Zwecke der Direktwerbung, insbesondere durch elektronische Post, zu schützen. Bei solchen Formen unerbetener Nachrichten zum Zweck der Direktwerbung ist es danach gerechtfertigt zu verlangen, die Einwilligung der Empfänger einzuholen, bevor ihnen solche Nachrichten gesandt werden.

Die Richtlinie ist bis zum 31. Oktober 2003 in nationales Recht umzusetzen. Aus der Entstehungsgeschichte der Richtlinie und den Erwägungsgründen lässt sich entnehmen, dass die beispielsweise von politischen oder wohltätigen Organisationen durchgeführte Anwerbung neuer Mitglieder oder Aufrufe zur Wahlunterstützung unter den Begriff der Direktwerbung fallen, also die Einwilligung erforderlich sein wird. Nachrichten zu anderen Zwecken, z. B. im Bereich allgemein bedeutsamer politischer Sachinformationen, werden vom Richtliniengeber wohl nicht als Direktwerbung angesehen. Mit der entsprechenden Grenzziehung wird sich der Bundesgesetzgeber bei der Umsetzung der Richtlinie zu befassen haben.

Die Position der Datenschutzbeauftragten sowohl auf nationaler als auch auf europäischer Ebene hierzu ist eindeutig: Sie werden für eine Stärkung des Einwilligungsmodells eintreten. Nur diese Lösung setzt nämlich das Grundrecht auf informationelle Selbstbestimmung konsequent um – erst fragen, dann handeln.

Im Idealfall gibt der Interessent an einem Newsletter seine eigenen Daten in dem Webformular auf der Internetseite (Homepage) der Abgeordneten ein, um den Newsletter zu erhalten. In diesem Falle ist er selbstverständlich mit der Nutzung seiner Daten zu diesem Zweck einverstanden. Um vollständige Transparenz zu schaffen, sollte der Nutzer vor der Absendung des Webformulars gem. § 4 Abs. 1 Teledienste-Datenschutzgesetz umfassend über die beabsichtigte Verarbeitung seiner personenbezogenen Daten informiert werden. In welchem Umfang hier sog. „Bestandsdaten“ (dies sind z. B. neben dem Namen die Anschrift, die Telefonnummer, das Geburtsdatum etc.) erhoben werden dürfen, ist am Grundsatz der Erforderlichkeit auszurichten. Daten, die zweckbedingt nicht zwingend erforderlich sind, dürfen nicht erhoben, verarbeitet oder genutzt werden. So dürfen bei der kostenlosen Bereitstellung von Informationen für die Allgemeinheit grundsätzlich keine Bestandsdaten erhoben werden, weil kein Vertragsverhältnis vorliegt und die Daten für die Abwicklung solcher Angebote nicht erforderlich sind. Dennoch werden bei kostenlosen Diensten wie der Bestellung von Newslettern von den Anbietern häufig neben der E-Mail-Adresse (für die Bestellung des Newsletters erforderlich) auch noch andere personenbezogene Daten erhoben. Dies ist in der Regel nicht zulässig, da diese Daten für die Erbringung der Leistung (Übersendung einer E-Mail) nicht notwendig sind.

Die Kommission beim Landesbeauftragten für den Datenschutz hofft, dass diese Ausführungen dazu beitragen, das Bewusstsein für den dargestellten Problembereich zu wecken.

Anlage 30

Orientierungshilfe
Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Zur Erreichung einer gemeinsamen Position befasste sich die in Trier tagende Herbstkonferenz der Datenschutzbeauftragten des Bundes und der Länder mit der datenschutzrechtlichen Beurteilung der kommunalen Speicherung und Veröffentlichung personenbezogener Standortverzeichnisse von Mobilfunkantennen. In der einstimmig hierzu verabschiedeten Entschließung fordern die Datenschützer aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung und Veröffentlichung von Mobilfunkkatastern zu entscheiden. Solange die geforderte bereichsspezifische Regelung fehlt, geht der Landesbeauftragte für den Datenschutz Rheinland-Pfalz von folgender Rechtslage aus:

1. Der Aufbau eines kommunalen Standortverzeichnisses ist datenschutzrechtlich dann zulässig, wenn dies zur Erfüllung einer in der Zuständigkeit der Kommunen stehenden Aufgabe erforderlich ist. Bei Berücksichtigung der aktuellen Verwaltungsrechtsprechung dürfte dies aufgrund der baurechtlichen Genehmigungsbedürftigkeit der Sendeanlagen gegeben sein.

2. Die Veröffentlichung der personenbezogenen Standortdaten im Internet ist mangels Rechtsgrundlage datenschutzrechtlich unzulässig. Insbesondere ist der individuelle antragsgebundene Auskunftsanspruch nach § 4 des Umweltinformationsgesetzes nicht geeignet, eine generelle Veröffentlichung der Daten – unabhängig vom Publikationsmedium – zu legitimieren.

3. Bei der Veröffentlichung personenbezogener Standortdaten auf lokaler Ebene außerhalb des Internets ist zu differenzieren:

   – Handelt es sich um sichtbare Sendeanlagen, ist die Information über den Antennenstandort ein allgemein zugängliches Datum. Dessen pauschale Veröffentlichung ist deshalb auf der Grundlage der §§ 2 Abs. 5 Satz 2; 16 Abs. 1 Nr. 2; 12 Abs. 4 Nr. 9 LDSG grundsätzlich zulässig. Denn bei sichtbaren Sendeanlagen steht der Veröffentlichung in der Regel kein überwiegendes schutzwürdiges Interesse der Betroffenen entgegen.

   – Bei verdeckten Sendeanlagen ist die Standortinformation nicht allgemein zugänglich. Eine Veröffentlichung der Daten wäre nur nach vorheriger Unterrichtung der Betroffenen über die bevorstehende Datenverarbeitung und das ihnen zustehende Widerspruchsrecht gemäß § 16 Abs. 1 Nr. 4 LDSG zulässig.

Anlage 31

Hinweise
zur datenschutzgerechten Gestaltung und Nutzung von E-Mail-Diensten durch öffentliche Stellen

Die elektronische Post (E-Mail) hat sich als Form des Austauschs und der Übertragung von Informationen in den Verwaltungen etabliert. Sie wird für die interne Kommunikation genutzt, für Mitteilungen an andere Behörden und im Verkehr mit dem Bürger; vielfach dient dabei das Internet als Kommunikationsmedium.

Aufgrund der technischen Gegebenheiten im Internet ist ein angemessener Schutz personenbezogener Daten häufig nicht gewährleistet. Die Vertraulichkeit der übertragenen Daten, ihre Vollständigkeit, Schutz vor unerlaubten Veränderungen (Integrität) sowie die verlässliche Zurechenbarkeit zu einem bestimmten Absender (Authentizität) müssen gegebenenfalls durch zusätzliche Maßnahmen sichergestellt werden.

Die datenschutzrechtlichen Anforderungen ergeben sich u. a. aus § 9 Abs. 2 Nr. 9 Landesdatenschutzgesetz (LDSG). Danach sind bei der Übetragung personenbezogener Daten via E-Mail Maßnahmen zu treffen, die gewährleisten, dass Nachrichten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Weitere datenschutzrechtliche Gesichtspunkte sind die Löschung von Nachrichten und die Protokollierung der E-Mail-Nutzung.

Die Datenschutzmaßnahmen sind in einer Dienstanweisung darzustellen (§ 9 Abs. 5 LDSG). Aus technisch-organisatorischer Sicht sind bei der Einführung von E-Mail-Verfahren die nachfolgenden Punkte zu berücksichtigen.[1)]

1. Organisatorische Festlegungen

Vor der Freigabe von E-Mail-Verfahren ist zu klären, in welchem Umfang die dienstliche Nutzung der elektronischen Post zugelassen wird. Ausschlaggebend sind die bestehenden Anforderungen an die Vertraulichkeit der Information, an deren Schutz vor unbefugter Veränderung und an die Verbindlichkeit einer Mitteilung (vgl. Nr. 3). Dabei ist festzulegen, in welchen Bereichen die elektronische Post ergänzend oder anstelle der Schriftform genutzt werden kann und in welchen Fällen Ausdrucke zu fertigen und zu den Akten zu nehmen sind. Ebenso wie für schriftliche Eingänge sind Vetretungsregelungen zu treffen (siehe Nr. 6).

Mailprogramme erlauben es meist, Absenderangaben wie Organisationsbezeichnung, Anschrift, Telefonnummer automatisch an das Ende einer E-Mail anzufügen. Soweit kein besonderer E-Mail-Briefkopf verwendet wird, sollte diese Möglichkeit genutzt werden, um die Zurechenbarkeit einer Nachricht zu unterstützen.

Die Adressierung beim Versand elektronischer Nachrichten muss so eindeutig erfolgen, dass fehlerhafte Zustellungen vermieden werden. Elektronische Nachrichten, die lediglich innerhalb einer öffentlichen Stelle versandt werden sollen, dürfen das interne Netz nicht verlassen. Hierauf ist insbesondere bei der Gestaltung beim Aufbau elektronischer Verteilerlisten zu achten.

2. Beschränkung auf die erforderlichen Komponenten und Dienste

Soweit lediglich die E-Mail-Funktionalität benötigt wird, sind ausschließlich die hierfür benötigten Komponenten bereitzustellen. Dies kann dadurch erfolgen, dass ein- und ausgehende Verbindungen über filternde Komponenten (z. B. Router) geleitet werden, die unzulässige Protokoll- und Diensteanforderungen zurückweisen. Falls die E-Mail-Anbindung im Rahmen eines mehrere Dienste umfassenden Internet-Zugangs realisiert wird, sind die Empfehlungen des LfD zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet zu berücksichtigen. [2)]

3. Verschlüsselung der Inhalte, digitale Signatur

Nachrichten der elektronischen Post werden, wenn keine besonderen Vorkehrungen zur Sicherung der Vertraulichkeit getroffen wurden, im Klartext übertragen. Sie können damit auf allen Systemen, über welche die Daten geleitet werden, mitgelesen oder verändert werden. Der Übertragungsweg und seine Eigenschaften sind dem Absender und dem Empfänger, vielfach auch dem Provider, beim E-Mail-Versand in der Regel weder bekannt noch durch sie beeinflussbar, eine Vertrauenswürdigkeit des Transportwegs ist damit nicht gegeben. Kryptographische Verfahren wie Verschlüsselung und digitale Signatur sind hier geeignet, Verletzungen

1) Vgl. – Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch
– Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Datenschutz bei elektronischen Mitteilungssystemen.
– Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 zur sicheren Übertragung personenbezogener Daten.

2) Orientierungshilfe „Anschluss von Netzen der öffentlichen Verwaltung an das Internet“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder.

des Datenschutzes bei der Übetragung schutzwürdiger Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler erkennen und die unberechtigte Kenntnisnahme unterbinden. Verschlüsselungs- und Signaturlösungen sind Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

Entsprechend der Sensibilität der übermittelten Daten ist daher bei der Nutzung öffentlicher Übertragungswege eine Verschlüsselung vorzusehen. Aus datenschutzrechtlicher Sicht gilt dies insbesondere für Fälle, in denen besondere Berufs- und Amtsgeheimnisse berührt sind (§ 203 Strafgesetzbuch). Hierbei sind als sicher anerkannte Verfahren mit ausreichender Schlüssellänge zu verwenden. Lösungen, die auf einer einfachen DES-Verschlüsselung oder einer effektiven Schlüssellänge von lediglich 40 Bit beruhen, genügen dem nicht. Geeignete Algorithmen sind z. B. Triple-DES mit 112 Bit oder IDEA mit 64 bzw. 128 Bit Schlüssellänge. Für asymmetrische Verfahren wie RSA wird ein Schlüssel von 1 024 Bit oder mehr empfohlen. Andere Lösungen kommen alternativ in Betracht, wenn diese nachweislich eine vergleichbare Sicherheit bieten. Bei personenbezogenen Daten geringer Sensibilität ist zumindest ein Schutz vor zufälliger Kenntnisnahme vorzusehen.

Für Verschlusssachen gelten die Regelungen der Verschlusssachenanweisung (VSA, MinBl. 1996 S. 66). Danach sind Verschlusssachen bei der Übertragung über technische Kommunikationsverbindungen mit zugelassenen Verfahren zu kryptieren bzw. durch andere zugelassene Maßnahmen zu sichern (VSA Nr. 47.1).

Für die verlässliche Zurechenbarkeit von Nachrichten und den Schutz vor unbefugten Veränderungen sollte daher auf digitale Signaturverfahren zurückgegriffen werden. Das in dieser Hinsicht mit einer zertifizierten Lösung nach dem Signaturgesetz (SigG) verbundene Schutzniveau kommt in der Regel nur dort in Betracht, wo besondere Anforderungen an Authentizität und Integrität elektronischer Daten bestehen und ein grundsätzlich offener Teilnehmerkreis vorliegt. Wenn regelmäßig ausschließlich festgelegte Stellen miteinander kommunizieren oder geringere Anforderungen an die Zurechenbarkeit und Unversehrtheit der Daten gestellt werden, sind aus Sicht des Datenschutzes auch andere Verfahren im Sinne des § 1 Abs. 2 SigG ausreichend.

Neben der Auswahl geeigneter Algorithmen ist beim Einsatz der Verfahren darauf zu achten, dass kein unbefugter Zugriff auf die verwendeten Schlüssel erfolgen kann. Soweit diese auf Festplatten oder Disketten gespeichert werden, sind sie durch geeignete Maßnahmen (z. B. Passphrase) entsprechend zu schützen.

4. Prüfung auf Schadensfunktionen in E-Mail-Anhängen

Nachrichten sind häufig Anlagen in Form von Dateien beliebigen Inhalts beigefügt. Diese können, vor allem, wenn es sich um lauffähige Programme, selbstextrahierende Dateien oder Dateien mit Makrofunktionen handelt, Schadensfunktionen enthalten. Vor der weiteren Verarbeitung sind daher die E-Mail-Eingänge mit aktuellen Prüfprogrammen regelmäßig auf sicherheitsrelevante Inhalte hin (Programm und Makroviren, Trojanische Pferde, ActiveX/Java-Komponenten usw.) zu untersuchen. Die Anwender sind darauf hinzuweisen, dass der Aufruf von E-Mail Anhängen, deren Schadensfreiheit nicht kontrolliert wurde, zu Problemen führen kann und unterbleiben soll.

5. Löschen von Nachrichten

Personenbezogene Nachrichten sind nach § 19 Abs. 2 LDSG zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Für die Speicherung verschickter und empfangener Nachrichten in den elektronischen Postfächern der Benutzer sowie auf dem Mail-Server der speichernden Stelle sind daher Regelungen über die Dauer der Speicherung zu treffen. Die daraus folgende Löschung nach Ablauf der festgelegten Speicherungsfrist sollte möglichst durch technische Maßnahmen unterstützt werden.

Die eingesetzten Programme für die E-Mail-Nutzung sind so zu konfigurieren, dass erfolgreich empfangene Nachrichten auf dem Mailserver des Providers gelöscht werden.
Im Hinblick auf die nach § 6 Abs. 2 Teledienstedatenschutzgesetz (TDDSG) vorgeschriebene Löschung von Nutzungs- und Abrechnungsdaten durch den Provider sollte im Rahmen des Vertragsschlusses eine entsprechende Bestätigung eingeholt werden.

6. Administration und Konfiguration der Mail-Systeme

Im Zusammenhang mit der o. g. Filterung von E-Mail-Verbindungen und der Prüfung auf sicherheitsrelevante Inhalte empfiehlt sich die Installation des lokalen Mail- bzw. Kommunikationsservers auf einem separaten Rechner. Die Verwaltung des Mail-Systems (postmaster) sollte aus Sicherheitsgründen von der Netzwerkverwaltung getrennt werden.

Der Verbindungsaufbau darf ausschließlich von der öffentlichen Stelle aus zum jeweiligen Provider möglich sein (Dial-up). Vorhandene Sicherheitsfunktionen der Anschlusskomponenten sind zu nutzen (vgl. Hinweise des LfD zur Einrichtung von ISDN-Wählverbindungen). Der Zugang zu den Postfächern der einzelnen Mitarbeiter oder Sachbereiche ist im Rahmen der Speicher- und Zugriffskontrolle nach § 9 Abs. 2 Nr. 3 und 5 LDSG durch geeignete Maßnahmen wie Benutzerpasswörter oder vergleichbare Lösungen (z. B. Chipkarte, Token) zu sichern.

Dies gilt auch für die lediglich vorübergehend benötigten Zugriffe im Vertretungsfall. Die Weiterleitung von Nachrichten im Vertretungsfall sollte nach Möglichkeit durch die Eingabe eines Abwesenheitszeitraums durch den Vertretenen und die damit verbundene automatische Zustellung an die jeweilige Vertretung erfolgen. Bei Inanspruchnahme der Vertretungsberechtigung muss im Rahmen der Eingabekontrolle erkennbar sein, dass nicht der eigentlich zuständige Bearbeiter, sondern die Vertretung zugegriffen hat.

7. Protokollierung der E-Mail-Nutzung

Nach § 9 Abs. 2 Nr. 6 LDSG ist im Rahmen der Übermittlungskontrolle zu gewährleisten, dass festgestellt werden kann, an wen welche personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können und dies einschließlich des Zeitpunktes stichprobenweise überprüft werden kann. Darüber hinaus kann eine Protokollierung für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs erfolgen. Hinsichtlich der Überwachung der ordnungsgemäßen Nutzung eines dienstlich bereitgestellten E-Mail-Zugangs bestehen gegen die Protokollierung

- des Versands von Nachrichten an gesperrte Empfängeradressen,
- des Versands/Empfangs von Nachrichten, die einen festgelegten Umfang überschreiten,
- des Versands/Empfangs von Massensendungen (Spam-Mail),
- des Empfangs von Nachrichten mit Schadensfunktionen (s. Nr. 4) sowie
- von Fehlermeldungen

keine Bedenken. Im Vordergrund steht dabei vor allem die Dokumentation sicherheitsrelevanter, auffälliger oder von allgemeinen Vorgaben abweichender Vorgänge. Bezüglich ihrer Nutzung unterliegen Protokolldaten einer engen Zweckbindung (§ 13 Abs. 5 LDSG). Ausdrücklich untersagt ist die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle (§ 31 Abs. 5 LDSG). Eine vollständige Aufzeichnung aller benutzerspezifischen Aktivitäten durch die Systembetreuung, insbesondere die grundsätzliche Speicherung der Inhalte elektronischer Post, ist im Allgemeinen nicht erforderlich. Beim Verdacht auf eine missbräuchliche Nutzung des E-Mail-Dienstes kann es notwendig werden, den Umfang der Protokollierung vorübergehend zu erweitern. Die Entscheidung hierüber sollte an der Häufigkeit und Bedeutung der aufzuklärenden Umstände orientiert und unter Beteiligung der Personalvertretung getroffen werden.

Inwieweit eine Protokollierung datenschutzrechtlichen Anforderungen entspricht, bemisst sich weiterhin nach der Dauer der Aufbewahrung der Protokolldaten und den bestehenden Zugriffs- und Auswertungsmöglichkeiten. Nach den Empfehlungen des LfD sollte die Aufbewahrungsdauer von Protokolldaten den Zeitraum eines Jahres nicht überschreiten. Soweit Protokolle zum Zweck gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsdauer vorzusehen; in der Regel reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

8. Veröffentlichung der E-Mail-Adressen der Angehörigen öffentlicher Stellen

Angaben über die elektronische Erreichbarkeit (Name, Amts- und Funktionsbezeichnung, dienstliche E-Mail-Adresse, öffentlicher Kryptografieschlüssel) unterliegen bei Angehörigen öffentlicher Stellen als Amtsträgerdaten nicht dem informationellen Selbstbestimmungsrecht. Gegen die Veröffentlichung dienstlicher E-Mail-Adressen bestehen daher aus datenschutzrechtlicher Sicht keine Bedenken. Dies beschränkt sich jedoch grundsätzlich auf Funktionsträger, die im Rahmen ihrer Aufgabenerfüllung nach außen hin tätig werden. Fürsorgegesichtspunkte können auch in diesen Fällen eine Beschränkung oder neutrale Fassung der Angaben erforderlich machen.

9. Private Nutzung

Gestattet der Dienstherr allgemein die private Nutzung eines vorhandenen E-Mail-Dienstes, wird er medienrechtlich zum Anbieter eine Teledienstes nach § 2 Abs. 2 Nr. 1 TDG und unterliegt den besonderen Anforderungen des Medienrechts an die Verarbeitung von Nutzungs- und Abrechnungsdaten. Mit der Erlaubnis zur privaten Nutzung der Kommunikationsanlage erbringt er weiterhin einen geschäftsmäßigen Telekommunikationsdienst gemäß § 3 Nr. 5 Telekommunikationsgesetz (TKG). Die private Nutzung des E-Mail-Dienstes unterliegt damit dem Fernmeldegeheimnis nach § 85 Abs. 2 TKG. Dieses erstreckt sich auf die Inhalte der Telekommunikation und ihre näheren Umstände.

Nach § 4 Abs. 2 Nr. 2 TDDSG hat der Diensteanbieter durch technisch-organisatorische Vorkehrungen sicherzustellen, dass die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist. Die Dauer der Speicherung von Abrechnungsdaten richtet sich nach § 6 Abs. 2 Nr. 2 TDDSG und beträgt bei Einzelnachweisen in der Regel 80 Tage nach Rechnungsversand. Die Nutzer sind nach § 3 Abs. 5 TDDSG über Art, Umfang, Ort und Zwecke der Verarbeitung personenbezogener Daten zu unterrichten.

Bei Vorliegen tatsächlicher Anhaltspunkte dürfen personenbezogene Daten der Nutzer für die Aufklärung einer missbräuchlichen Inanspruchnahme des Dienstes ermittelt werden (vgl. Nr. 7). In der Dienstanweisung sollte daher festgelegt werden, ob und ggf. mit welchen Einschränkungen eine private Nutzung zugestanden wird.

Angesichts der unterschiedlichen medienrechtlichen Anforderungen an die dienstliche und private E-Mail-Nutzung sollte letztere über einen separaten Account erfolgen und anhand eines unterschiedlichen Adressierungsschemas unterscheidbar sein (z. B. name.privat@dienststelle.de). Dies dient auch der in den Telekommunikationsanschlussvorschriften des Landes geforderten getrennten Erfassung der privaten Nutzung (VV FM Nr. 2.3.1, MinBl. 1998 S. 119).

10. Anmeldung zum Datenschutzregister; Geräte- und Verfahrensverzeichnis

Soweit im Rahmen der E-Mail-Kommunikation personenbezogene Daten verarbeitet werden, besteht eine Anmeldepflicht nach § 27 LDSG. Das Verfahren und die eingesetzten Programme sind in das Geräte- und Verfahrensverzeichnis nach § 10 Abs. 2 und 3 LDSG aufzunehmen.

Für die Anmeldung zum Datenschutzregister gelten die im 16. Tätigkeitsbericht des LfD, Tz. 21.8.3 genannten Kriterien. Aus einer E-Mail-Anbindung ergeben sich Risiken für die angeschlossenen IT-Systeme. Soweit auf diesen meldepflichtige Verfahren nach § 27 LDSG betrieben werden, stellt dies eine wesentliche Änderung der technischen Rahmenbedingungen dar, die dem LfD mitzuteilen ist. Ausreichend ist die einmalige Anmeldung des Verfahrens unter Angabe der Zahl der angeschlossenen Arbeitsplätze und Mail-Server. Anmeldungen für die einzelnen Rechner sind nicht erforderlich.

Anlage 32

Checkliste „Automatisierte Einzelentscheidung“ gem. § 5 Abs. 5 LDSG
(Stand: Juli 2002)

Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient.

1. Werden personenbezogene Daten verarbeitet, die der Bewertung einzelner Persönlichkeitsmerkmale dienen?
   Beispielsweise fallen darunter Beurteilungsnoten, Examensergebnisse, Kreditwürdigkeitsfaktoren u. Ä.

   Nein: O Dann gilt das Verbot der automatisierten Einzelentscheidung des § 5 Abs. 5 nicht.
   Ja: O Weiter mit Frage 2.

2. Werden auf der Basis dieser Daten Entscheidungen gefällt, die für die Betroffenen rechtlich relevant sind?

   Nein: O Weiter mit Frage 3.
   Ja: O Weiter mit Frage 4.

3. Werden auf der Basis dieser Daten Entscheidungen gefällt, die die Betroffenen erheblich beeinträchtigen?

   Nein: O Dann gilt das Verbot der automatisierten Einzelentscheidung des § 5 Abs. 5 nicht.
   Ja: O Weiter mit Frage 4.

4. Besteht zwischen der automatisierten Datenauswertung und der Entscheidung ein Automatismus?
   (Fehlt vor der Entscheidung eine ergänzende Prüfung durch eine Person?)

   Nein: O Dann handelt es sich nicht um eine automatisierte Einzelentscheidung im Sinne des § 5 Abs. 5.
   Ja: O Weiter mit Frage 5.

5. Ergeht die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses und wird dem Begehren der Betroffenen stattgegeben?

   Ja: O Dann gilt das Verbot der automatisierten Einzelentscheidung des § 5 Abs. 5 nicht.
   Nein: O Weiter mit Frage 6.

6. Wird die Wahrung der berechtigten Interessen der Betroffenen durch geeignete Maßnahmen gewährleistet und wird den Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer rechtlich relevanten oder erheblich beeinträchtigenden Entscheidung mitgeteilt?

   (Als geeignete Maßnahme gilt insbesondere die Möglichkeit der Betroffenen, ihren Standpunkt geltend zu machen mit der Folge, dass die verantwortliche Stelle ihre Entscheidung erneut vollinhaltlich prüft.)

   Ja: O Dann gilt das Verbot der automatisierten Einzelentscheidung des § 5 Abs. 5 nicht.
   Nein: O Dann ist die beabsichtigte Nutzung des Verfahrens unzulässig.

Anlage 33

Checkliste Benachrichtigung der Betroffenen gem. § 18 Abs. 1 LDSG
(Stand: Februar 2001)

Besteht gem. § 18 Abs. 1 eine Benachrichtigungspflicht gegenüber den Betroffenen?

1. Werden Daten ohne Kenntnis der Betroffenen erhoben?

   Nein: O Dann besteht keine Benachrichtigungspflicht.
   Ja: O Weiter mit Frage 2.

2. Haben die Betroffenen auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt?

   Ja: O Dann besteht keine Benachrichtigungspflicht.
   Nein: O Weiter mit Frage 3.

3. Ist die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen?

   Ja: O Es besteht dann keine Benachrichtigungspflicht, wenn die unter Punkt 7 angesprochene schriftliche Festlegung getroffen wurde.
   Nein: O Weiter mit Frage 4.

4. Würde die Unterrichtung der Betroffenen einen unverhältnismäßigen Aufwand erfordern?

   Ja: O Begründung beispielsweise: Zahl der Betroffenen ist immens/geringe Sensitivität der erhobenen Daten/zu begründendes geringes Informationsinteresse der Betroffenen/sonstige Gründe;
   es besteht dann keine Benachrichtigungspflicht, wenn die unter Punkt 7 angesprochene schriftliche Festlegung getroffen wurde.
   Nein: O Die Betroffenen sind zu benachrichtigen.

5. Inhalt der Benachrichtigung:

   Die Betroffenen sind über die Speicherung, die Identität der verantwortlichen Stelle, das Bestehen von Auskunfts- und Berichtigungsrechten sowie über die Zweckbestimmung der Datenverarbeitung zu unterrichten. Sie sind auch über die empfangenden Stellen oder über die Kategorien von empfangenden Stellen zu unterrichten, soweit sie nicht mit der Übermittlung an diese rechnen müssen. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

6. Wie wird dieser Pflicht entsprochen?

   O Durch eine schriftliche ausdrückliche Benachrichtigung?
   O In sonstiger Weise?

7. Hat die verantwortliche Stelle schriftlich festgelegt (gem. § 18 Abs. 2 Satz 2), unter welchen Voraussetzungen von einer Unterrichtung wegen der Erhebung auf gesetzlicher Grundlage (s. o. 3.) oder zu großen Aufwandes (s. o. 4.) abgesehen werden kann?

Anlage 34

Checkliste „Vorabkontrolle“, § 9 Abs. 5 LDSG
(Stand: Juli 2002)

Soweit Verfahren automatisierter Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Aus den Ausnahmen zum Erfordernis der Vorabkontrolle, die den Fragen 1 bis 6 zugrunde liegen, ergibt sich, dass die Vorabkontrolle in erster Linie eine Rechtskontrolle ist. Ergeben sich Zweifel an der Rechtmäßigkeit geplanter Verarbeitungsverfahren, hat sich der behördliche Datenschutzbeauftragte an die zuständige Aufsichtsbehörde zu wenden.

Inhaltlich beruht die Vorabkontrolle auf einer besonderen Prüfung der für die automatisierte Verarbeitung maßgebenden Gesichtspunkte. Dazu gehören neben der Prüfung der Rechtmäßigkeit vor allem die Durchführung vorgeschriebener Beteiligungen und Unterrichtungen, die verfahrensmäßige Abbildung von Rechten der Betroffenen, die Einhaltung formaler Anforderungen sowie erforderliche technisch-organisatorische Maßnahmen.

Prüfpunkte, ob überhaupt eine Vorabkontrolle erforderlich ist

1. Werden besondere Arten personenbezogener Daten verarbeitet?
   Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 3 Abs. 9 LDSG).

   Nein: O Weiter mit Frage 2.
   Ja: O Weiter mit Frage 4.

2. Ist die Verarbeitung personenbezogener Daten dazu bestimmt, die Persönlichkeit der Betroffenen zu bewerten einschließlich ihrer Fähigkeiten, ihrer Leistung oder ihres Verhaltens?

   Nein: O Weiter mit Frage 3.
   Ja: O Weiter mit Frage 4

3. Weist das vorliegende Verfahren aus sonstigen Gründen besondere Risiken für die Rechte und Freiheiten der Betroffenen auf?

   Nein: O Dann ist keine Vorabkontrolle erforderlich.
   Ja: O Weiter mit Frage 4.

4. Beruht die Datenverarbeitung auf einer gesetzlichen Verpflichtung?

   Ja: O Auf §§ ……. ;
   -> dann ist die Prüfung beendet, eine Vorabkontrolle ist nicht erforderlich.

   Nein: O Weiter mit Punkt 5.

5. Liegt eine Einwilligung der Betroffenen vor?

   Ja: O (Anforderungen an die Einwilligung gemäß § 5 Abs. 2 bis 4 LDSG: Aufklärung, Hinweis auf Widerruf, Schriftform, ausdrücklicher Bezug auf die besonderen Datenarten),
   -> dann ist die Prüfung beendet, eine Vorabkontrolle ist nicht erforderlich.

   Nein: O Weiter mit Punkt 6.

6. Dient die Verarbeitung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen?

   Ja: O Folgende Rechtsbeziehungen bestehen zu den Betroffenen:
   ……
   -> dann ist die Prüfung beendet, eine Vorabkontrolle ist nicht erforderlich.

   Nein: O Weiter mit Frage 7.

7. Beruht die Datenverarbeitung auf einer gesetzlichen Ermächtigung?

   Ja: O Auf §§ …….;
   Nein: O -> dann ist die Datenverarbeitung unzulässig.

Inhalt der Vorabkontrolle

8. Materielle Anforderungen

   Ist die Datenverarbeitung verhältnismäßig (erforderlich, geeignet und angemessen)?

   Wird der Grundsatz der Datensparsamkeit und Datenvermeidung (§ 1 Abs. 3 LDSG) beachtet?
   - Ist eine Datenverarbeitung mit anonymisierten Daten möglich?
   - Wenn nein: Ist eine frühestmögliche Anonymisierung vorgesehen?
   - Kann eine Pseudonymisierung erfolgen?

   Sind die Rechte der Betroffenen nach § 6 I LDSG berücksichtigt?

   Zum Beispiel:
   - Kann einem Auskunftsersuchen nach § 18 Abs. 3 LDSG angemessen entsprochen werden?
   - Können Daten erforderlichenfalls nach § 19 Abs. 3 gesperrt werden?
   - Sind Löschungsfristen vorgegeben (§ 19 Abs. 2 Nr. 2) und ist verfahrensmäßig sichergestellt, dass diese eingehalten werden?
   - Sind ggf. die Vorgaben einer Auftragsdatenverarbeitung nach § 4 LDSG berücksichtigt?
   - Sind ggf. geeignete Maßnahmen gemäß § 5 Abs. 5 Nr. 2 LDSG getroffen und ist verfahrensmäßig sichergestellt, dass die Unterrichtung der Betroffenen erfolgt ?

9. Formale Anforderungen

   Ist das Verfahren in das Verfahrensverzeichnis aufgenommen (§ 10 Abs. 2 LDSG)?

   Ist gegebenenfalls – bei einem automatisierten Abrufverfahren – eine Anhörung des LfD nach § 7 Abs. 3 LDSG erfolgt?

   Wurden gegebenenfalls – bei einem automatisierten Abrufverfahren – erforderliche Zulassungen (z. B. § 7 Abs. 3 und 5 LDSG) erteilt?

   Wurde die Verpflichtung auf das Datengeheimnis nach § 8 Abs. 2 LDSG vorgenommen?

   Liegt für das Verfahren eine Dienstanweisung über die techn.-org. Datenschutzanforderungen nach § 9 Abs. 6 LDSG vor?

10. Technisch-organisatorische Anforderungen

    § 9 Abs. 2 Satz 2 LDSG sieht technisch-organisatorische Sicherungsmaßnahmen generell vor, soweit personenbezogene Daten automatisiert verarbeitet werden. Im Rahmen der Vorabkontrolle ist in diesem Zusammenhang daher zu prüfen, ob die sich aus dem Verfahren ergebenden besonderen Risiken zusätzliche Maßnahmen erfordern und in welcher Weise dem entsprochen wird.

    Beruhen die besonderen Risiken auf der Art der Daten (§ 9 Abs. 5 Nr. 1 LDSG)?

    Wenn ja, -> sind Maßnahmen insbesondere im Bereich Zugriffs-, Weitergabe-, Eingabe-, Dokumentations- und Verarbeitungskontrolle nach § 9 Abs. 2 LDSG getroffen?

    Welche .....

    Beruhen die besonderen Risiken auf der Zweckbestimmung der Verarbeitung (§ 9 Abs. 5 Nr. 2 LDSG)?

    Wenn ja, -> sind Maßnahmen insbesondere im Bereich der Zweckbindungs-, Dokumentations- und Verarbeitungskontrolle nach § 9 Abs. 2 LDSG getroffen?

    Welche .....

11. Ergebnis der Vorabkontrolle

    Der behördliche Datenschutzbeauftragte hat am ..... festgestellt:

    Die Prüfung hat ergeben, dass die beabsichtigte Datenverarbeitung akzeptiert werden kann.

Anlage 35

Europäische Konferenz der Datenschutzbeauftragten
vom 9. bis 11. September 2002 in Cardiff (Wales/Großbritannien)

Erklärung zur zwangsweisen systematischen Speicherung von Verkehrsdaten der Telekommunikation vom 11. September 2002

Die Europäischen Datenschutzbeauftragten haben mit Sorge festgestellt, dass in der dritten Säule der Europäischen Union Vorschläge erörtert werden, die zur zwangsweisen systematischen Speicherung von Verkehrsdaten über alle Arten der Telekommunikation (d. h. detaillierte Angaben über die Zeit, den Ort und die benutzten Rufnummern bzw. Kennungen für Telefon, Fax, E-Mail und andere Nutzungsformen des Internets) für einen Zeitraum von einem Jahr oder länger führen würden, um Strafverfolgungs- und Sicherheitsbehörden den möglichen Zugang zu erlauben. Die Europäischen Datenschutzbeauftragten haben gravierende Zweifel hinsichtlich der Legitimität und Legalität derart weitreichender Maßnahmen. Sie weisen auf die erheblichen Kosten, die für die Telekommunikations- und Internetwirtschaft entstehen würden, wie auch auf die Tatsache hin, dass nicht einmal in den Vereinigten Staaten derartige Maßnahmen vorgesehen sind. Wiederholt haben die Europäischen Datenschutzbeauftragten betont, dass eine solche Vorratsdatenspeicherung ein unzulässiger Eingriff in die Grundrechte des Einzelnen nach Artikel 8 der Europäischen Menschenrechtskonvention wäre, wie dies der Europäische Menschenrechtsgerichtshof näher ausgeführt hat (siehe die Stellungnahme 4/2001 der Artikel 29-Arbeitsgruppe nach Richtlinie 95/46/EG, und die Erklärung der Europäischen Datenschutzkonferenz in Stockholm vom April 2000).

Der Schutz von Telekommunikationsverkehrsdaten ist jetzt auch geregelt durch die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates hinsichtlich des Schutzes der Privatsphäre in der elektronischen Kommunikation (Amtsblatt L 201/37), nach der die Verarbeitung von Verkehrsdaten im Grundsatz für Abrechnungszwecke zugelassen ist. Nach langer und gründlicher Debatte muss die Aufbewahrung von Verkehrsdaten für Zwecke der Strafverfolgung den strengen Vorgaben des Artikels 15 Abs. 1 der Richtlinie genügen: Das heißt, in jedem Fall ist sie nur zulässig für eine begrenzte Zeitspanne und wo dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Wenn Verkehrsdaten in bestimmten Fällen gespeichert werden sollen, muss dafür eine nachweisliche Notwendigkeit bestehen, die Dauer der Speicherung muss so kurz wie möglich sein und das Verfahren muss durch Gesetz eindeutig und in einer Weise geregelt sein, die hinreichende Sicherungen gegen unberechtigten Zugriff und jeden anderen Missbrauch vorsieht. Die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger wäre eindeutig unverhältnismäßig und deshalb in jedem Fall inakzeptabel.

Die Europäischen Datenschutzbeauftragten erwarten, dass die Artikel 29-Arbeitsgruppe Gelegenheit zur Stellungnahme zu Maßnahmen erhält, die sich aus den Diskussionen in der dritten Säule ergeben, bevor sie beschlossen werden.