



Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Landesbeauftragte für den Datenschutz NRW
Postfach 20 04 44, 40102 Düsseldorf

Herrn
Landtagspräsident
Ulrich Schnidt, MdL
Platz des Landtags 1

40221 Düsseldorf



Reichsstraße 43, 40217 Düsseldorf
E-Mail: datenschutz@lfd.nrw.de
Bearbeitung: **Frau Siekmann**
Durchwahl (0211) 38 424 - **93**
Aktenzeichen
L 5.4.2

- Aktenzeichen bitte unbedingt angeben -

18. Februar 2003

16. Datenschutzbericht 2003 der Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident,

nach § 27 Datenschutzgesetz für das Land Nordrhein-Westfalen (DSG NRW) lege ich dem Landtag den 16. Datenschutzbericht für die Zeit vom 01.01.2001 bis zum 31.12.2002 vor.

Die für die Mitglieder des Landtags bestimmten Exemplare sind beigefügt.

Mit freundlichen Grüßen

Sokol

(Sokol)

Datenschutzbericht 2003



Die Landesbeauftragte
für den Datenschutz
und Beauftragte für das
Recht auf Information
Nordrhein-Westfalen

Sechzehnter Datenschutzbericht

der

Landesbeauftragten für den Datenschutz und

Beauftragten für das Recht auf Information

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 2001
bis zum 31. Dezember 2002

Herausgeberin:

Die Landesbeauftragte für den Datenschutz und
Beauftragte für das Recht auf Information
Nordrhein-Westfalen
Bettina Sokol
Reichsstraße 43

40217 Düsseldorf

Tel: 0211/38424-0
Fax: 0211/38424-10
E-Mail: datenschutz@lfd.nrw.de

Diese Broschüre kann unter www.lfd.nrw.de oder
www.nordrhein-westfalen.datenschutz.de abgerufen werden.

ISSN: 0179-2431
Druck: Schäfer Druck GmbH
Düsseldorf 2003

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorbemerkung		1
1	**Zur Situation im Datenschutz - transparentere Verwaltungen**	2
2	**Medien**	8
2.1	Entwicklung des medienrechtlichen Rahmens	8
2.2	eGovernment: Nur mit Datenschutz ein Serviceangebot an Bürgerin und Bürger	10
2.3	Onlineangebote von Kommunen - Nachbesserungsbedarf beim Datenschutz	11
2.4	Neue Regelungen zur Überwachung	12
2.4.1	Der Staat hört mit - Telekommunikations-Überwachungs-verordnung	12
2.4.2	Cyber Crime Convention - Kriminalitätsbekämpfung um jeden Preis?	14
2.4.3	Protokollierung der Daten bei den Providern	15
2.4.4	Überwachung wird mobil	16
2.5	Presse - genügt freiwillige Selbstkontrolle für einen effektiven Datenschutz?	17
2.6	Einzelfragen zu Telekommunikation, Internet und E-Mail	18
2.6.1	Aufnahme in elektronische oder gedruckte Telefonverzeichnisse	18
2.6.2	Spamming und Newsletter	19
2.6.3	Elektronische Formulare	21
2.6.4	Internet-Cafés	22
2.6.5	Chats und Foren	23
3	**Technik**	25
3.1	Ferngesteuerte Internetanbindung	25
3.2	Biometrie - ein Allheilmittel zur Identifikation?	28
3.3	Sicherheitsanforderungen an Medizinnetze	31

3.3.1	Formen der Datenhaltung	31
3.3.2	Spezielle Datensicherheitsmaßnahmen	32
3.4	Allzeit bereit - Risiken mobiler Kommunikation	39
3.5	Einzelfragen zur Datensicherheit	44
3.5.1	Outsourcing von Verwaltungsnetzen	44
3.5.2	Anwendungsfehler: Kleine Ursache - großer Schaden für den Datenschutz	45
3.5.3	Datensicherheit auf FTP-Servern	46
3.5.4	Alle Jahre wieder	46
4	**Neues Bundesdatenschutzgesetz**	49
5	**Videoüberwachung**	55
6	**Wohnen und Liegenschaften**	60
6.1	Warndatei im Wohnungswesen	60
6.2	Mietbewerbungsbogen und Selbstauskünfte	62
6.3	Geobasisdaten - Informationssysteme offen für kommerzielle Nutzung?	64
6.4	Luftbildaufnahmen von Gebäuden und Grundstücken	65
6.5	Denkmalliste im Internet	68
6.6	Veröffentlichung von Bodenbelastungsdaten in Karten	69
7	**Verkehr**	71
7.1	TÜV Service Card - Service oder aufgedrängte Kundenbindung?	71
7.2	Schüler-Schoko-Ticket mit bitterem Beigeschmack	71
7.3	Elektronisches Fahrgeldmanagement	72
7.4	Aufzeichnung von Telefongesprächen im Flughafenbetrieb	73
7.5	Scannen von Passdaten beim Check-In	74
7.6	„Miles & More" - Kundenbindungsprogramm einer Fluggesellschaft	75
8	**Handel, Auskunfteien und Kreditwirtschaft**	77
8.1	Verwendung von Personalausweisen bei Banken, im Handel und für Selbstauskünfte bei Auskunfteien	77

8.2	Verbraucherschutz durch Information	79
8.3	Handel	81
8.3.1	Abwehr unerwünschter Werbezuschriften	81
8.3.2	Bezahlung mit EC-Karte	84
8.3.3	Kundenbindungsprogramme - weit mehr als ein elektronisches Rabattsystem	85
8.3.4	Zusatzfunktion auf dem Geldkartenchip für den Jugendschutz	87
8.4	Auskunfteien	89
8.4.1	Auskunftsanspruch nach dem neuen Bundesdatenschutzgesetz	89
8.4.2	Scoringverfahren der SCHUFA	91
8.4.3	Zeitdauer der Auskunft: „Bestrittene Daten in Prüfung"	93
8.4.4	Nachbarschaftsbefragungen	93
8.4.5	Vom mittelalterlichen Marktplatz ins Internet: Pranger- und Warndateien	94
8.5	Kreditwirtschaft	96
8.5.1	Auswertung des Überweisungsverkehrs zu Werbezwecken	96
8.5.2	Absenkung des Schwellenbetrages nach dem Geldwäschegesetz in der Euro-Umtauschphase	97
9	**Beschäftigte und Arbeitsorganisation**	99
9.1	Dienstliche und private Nutzung von E-Mail und Internet am Arbeitsplatz	99
9.2	Überwachung am Arbeitsplatz	102
9.3	Qualitätsmanagement bei der Polizei	106
9.4	Outsourcing der Beihilfe	107
9.5	Datenschutz im Personalrat	109
10	**Vereine**	110
10.1	Veröffentlichung von Mitgliederdaten im Internet	110
10.2	Übermittlung von Mitgliederdaten an Sponsoren	110
11	**Bildung und Forschung**	113
11.1	Schulen ans Netz	113

11.2	Modell „Selbständige Schule" - aber bitte ohne Fiasko für den Datenschutz	114
11.3	Information an Eltern volljähriger Schülerinnen und Schüler	115
11.4	Mangelhafte Personalaktenführung bei oberen Schulaufsichtsbehörden	117
11.5	Genealogische und zeitgeschichtliche Forschung	119
11.6	Forschung mit Blut- und Gewebeproben	121
12	**Kommunales**	124
12.1	Bekanntgabe personenbezogener Daten in der Kommunalverwaltung	126
12.2	Meldebescheinigung auch für einen einzigen Zweck	127
12.3	Datenübermittlung für die Kindergartenbedarfsplanung	128
12.4	Datenschutzgerechte Ausgestaltung von Bürgerbüros	128
13	**Soziales**	130
13.1	Neue Formulare im Sozialbereich	132
13.2	Umorganisation der Versorgungsverwaltung - Nachholbedarf beim Datenschutz	133
13.3	Call-Center einer gesetzlichen Krankenkasse	133
13.4	Schweigepflichtentbindungserklärung von privaten Versicherungen	135
14	**Gesundheit**	139
14.1	Datenpool am Swimmingpool	140
14.2	Krankenhausentlassungsberichte an Krankenkassen	141
14.3	Kundendateien in Apotheken	141
14.4	Patientendatenmissbrauch durch Apotheken und deren Rechenzentren	145
15	**Ausländerinnen und Ausländer**	148
16	**Polizei**	150
16.1	Opferschutz im Polizeigesetz	155
16.2	Unfallnachsorge bei Straßenverkehrsunfällen	155

16.3	Ordnungspartnerschaft zwischen Polizei und privaten Sicherheitsdiensten	156
16.4	Nur noch bargeldlose Zahlung von Verwarnungsgeldern - Anonymität dahin?	158
17	**Justiz**	160
17.1	Freiwillig in die DNA-Analyse-Datei?	162
17.2	Muss eigentlich jeder Brief gelesen werden?	164
17.3	Erfassung von Besucherdaten	165
17.4	Elektronische Datenverarbeitung bei den Gerichten	166
18	**Rechtsanwältinnen und Rechtsanwälte**	170
19	**Finanzen**	172
19.1	Information über Daten zur eigenen Person	172
19.2	Durchsuchungen bei Dritten	173
20	**Statistik**	175
20.1	Zensustestgesetz	175
20.2	Zählung des Verkehrsaufkommens	176
21	**Behördliche und betriebliche Datenschutzbeauftragte**	178
21.1	Datenschutzbeauftragte bei öffentlichen Stellen	178
21.2	Betriebliche Datenschutzbeauftragte	182
22	**Das neue Informationsfreiheitsgesetz**	183
22.1	Zur „Sicherstellung" des Rechts auf Information	183
22.2	Streit um die Gesetzesanwendung	185
22.3	Vorrang anderer Rechtsvorschriften über den Zugang zu Informationen	186
22.4	Beratung und Begründungspflicht im Verfahren	188
22.5	Zu den Verweigerungsgründen	191
22.5.1	Verweigerung des Informationszugangs bei laufenden Verfahren	191
22.5.2	Schutz des Entscheidungsbildungsprozesses	191
22.5.3	Schutz von Betriebs- oder Geschäftsgeheimnissen	194

22.5.4	Öffentliche Auftragsvergabe und Informationszugangsrecht	196
22.5.5	Schutz personenbezogener Daten	197
22.6	Veröffentlichung von Geschäftsverteilungsplänen. Schutz von Beschäftigtendaten	200
22.7	Kosten für den Informationszugang	200
Anhang		202
61. Konferenz am 08./09. März 2001		202
1.	Novellierung des G 10-Gesetzes	202
2.	Datenschutz bei der Bekämpfung von Datennetzkriminalität	203
3.	Novellierung des Melderechtsrahmengesetzes	205
Entschließungen zwischen den Konferenzen		206
4.	Veröffentlichung von Insolvenzinformationen im Internet (24. April 2001)	206
5.	Entwurf der Telekommunikations-Überwachungsverordnung (10. Mai 2001)	208
6.	Datenschutzrechtliche Grundanforderungen an die Videoüberwachung in öffentlichen Verkehrsmitteln (05.10.2001)	209
62. Konferenz vom 24. – 26. Oktober 2001		211
7.	EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft	211
8.	Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen	213
9.	Lkw-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen	215
10.	Datenschutzrechtliche Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte)	217
11.	„Neue Medienordnung"	219
12.	Gesetzliche Regelung von genetischen Untersuchungen	219
63. Konferenz am 07./08. März 2002		221
13.	Biometrische Merkmale in Personalausweisen und Pässen	221
14.	Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten	222
15.	Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz	223
16.	Neues Abrufverfahren bei den Kreditinstituten	224

Entschließung zwischen den Konferenzen 225
17. Geplanter Identifikationszwang in der Telekommunikation (24. Mai 2002) 225
64. Konferenz am 24./25. Oktober 2002 227
18. Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen 227
19. Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet 227
20. Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht 229
Entschließung der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) 229
Korruptionsbekämpfung durch Informationsfreiheit (20. November 2002) 229
Stichwortverzeichnis 231
Bestellformular Informationsmaterial

Vorbemerkung

Der Berichtszeitraum ist wieder einmal von grundlegenden Veränderungen gekennzeichnet. Neben der Zuständigkeit für den Datenschutz obliegt der Dienststelle seit dem 01. Januar 2002 ebenfalls die Kontrolle der Einhaltung des neuen Informationsfreiheitsgesetzes. Auch diese neue Aufgabe ist sehr spannend und wurde mit großer Freude zusätzlich übernommen.

Die Arbeitsbelastung der Dienststelle - auch dies muss einmal offen angesprochen werden - hat sich in den letzten Jahren allerdings stetig und in großem Umfang erhöht. Gegenüber 1999 hat sich beispielsweise allein die Anzahl der im Jahre 2002 eingegangenen schriftlichen Beschwerden und Anfragen - von den telefonischen ganz zu schweigen - mehr als verdoppelt. Die Kontroll- und Beratungstätigkeit ist zudem teilweise mit einem hohen Zeitaufwand verbunden, insbesondere wenn es etwa um groß angelegte, komplexe Projekte geht, die rechtlich und technisch beraten werden wollen. Dass die zu erledigende Arbeit mit dem vorhandenen Personal bei aller Kraftanstrengung nicht zu schaffen ist, wurde auch durch eine Organisationsuntersuchung bestätigt. Ein großes Beratungsunternehmen aus der freien Wirtschaft hat uns fast ein halbes Jahr lang bei unserer Tätigkeit begleitet und uns für die fachliche Arbeit im Ergebnis einen Mehrbedarf von zehn Personen bescheinigt. Die angespannte Personalsituation bringt es außerdem leider mit sich, dass auch die Beantwortung der datenschutzrechtlichen Anliegen nicht immer so zeitnah erfolgen kann, wie wir alle es uns wünschen. Für das hohe Engagement, mit dem meine Mitarbeiterinnen und Mitarbeiter trotz dieser widrigen Umstände die Arbeit erledigen, sei Ihnen auch öffentlich ganz herzlich gedankt.

Im Berichtszeitraum konnten gemeinsam mit dem Institut für Informations-, Telekommunikations- und Medienrecht sowie dem Institut für Kriminalwissenschaften an der Universität Münster ebenfalls wieder zwei sehr gut besuchte Symposien veranstaltet werden. Das Für und Wider des Verordnungsentwurfs für eine Telekommunikations-Überwachungsverordnung (TKÜV) war Gegenstand des Symposiums „Die neue TKÜV - Innere Sicherheit auf Kosten von Netzbürgern und Providern?". Mit den Problemen der DNA-Analyse und weitergehend mit dem Umgang mit genetischen Daten im Arbeits- und Wirtschaftsleben befasste sich das Symposium „Der gläserne Mensch - DNA-Analysen, eine Herausforderung an den Datenschutz".

1 Zur Situation im Datenschutz - transparentere Verwaltungen

Mehr Licht! Schon im 13. Datenschutzbericht 1995/96 wurde dargestellt, dass in einer zeitgemäßen Datenschutzkonzeption auch ein allgemeines Informationszugangsrecht seinen Platz hat. Dieser Wunsch ist mittlerweile in Erfüllung gegangen. Anfang 2002 ist das **Informationsfreiheitsgesetz** NRW (IFG NRW) in Kraft getreten. Seitdem kann sich jede Person ohne weitere Begründung über die bei den öffentlichen Stellen vorhandenen Unterlagen informieren - dies selbstverständlich unter Wahrung des Schutzes personenbezogener Daten, also des Rechts auf informationelle Selbstbestimmung.

Nach den bisherigen Erfahrungen geraten Datenschutz und Informationsfreiheit in der Regel nicht miteinander in Konflikt. Die Menschen wollen von den Verwaltungen entweder etwas über die zu ihrer eigenen Person gespeicherten Daten wissen - worauf sie nach dem Landesdatenschutzgesetz schon immer einen Anspruch hatten. Oder sie interessieren sich für Vorgänge, in denen schützenswerte personenbezogene Daten ohnehin nicht enthalten sind oder leicht unkenntlich gemacht werden können.

Damit wird auch deutlich, dass **Datenschutz und Informationsfreiheit** grundsätzlich **keinen Widerspruch** darstellen, sondern vielmehr in einer engeren Verbindung stehen als gemeinhin angenommen wird. In seiner Volkszählungsentscheidung von 1983 benennt das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung als eine elementare Funktionsbedingung „eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens" (BVerfGE 65, 1-43). Ein wesentliches Ziel des Rechts auf informationelle Selbstbestimmung besteht daher darin, die Kommunikations- und Handlungsfähigkeit der einzelnen Menschen gegenüber staatlichen Stellen wie auch innerhalb der Gesellschaft sicherzustellen. Gerade unter den Bedingungen der Informations- und Wissensgesellschaft wird die Informationsfreiheit damit gleichsam zu einer der tatsächlichen Voraussetzungen für eine effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Informationszugangsrechte und Datenschutz haben also das gemeinsame Ziel, staatlicher Informationsmacht Grenzen zu setzen.

Da mir zusätzlich zum Datenschutz die Funktion der Landesbeauftragten für Informationsfreiheit übertragen worden ist, wenden sich Bürgerinnen und Bürger, deren Informationsanträge abgelehnt wurden, an meine Dienststelle mit der Bitte um Unterstützung ihrer Anliegen. Auch manche öffentlichen Stellen möchten gewisse Rechtsunsicherheiten beim Umgang mit dem neuen Gesetz lieber vorab geklärt wissen. Da bei uns also nur die „Problemfälle" landen, kann die Gesamtzahl der im Lande gestellten Informationsanträge von hier nicht verlässlich beurteilt werden. Das Gesetz sieht eine Gesamterhebung und Evaluation nach zwei Jahren vor. Allerdings ist bei aller Vorsicht schon jetzt erkennbar, dass die Menschen von ihrem neuen Recht durchaus regen Gebrauch machen.

Das Gegenteil einer Begrenzung staatlicher Informationsmacht findet allerdings seit dem 11. September 2001 auf anderen Gebieten statt. Die Terroranschläge wurden zum Anlass genommen, ein ganzes **Bündel gesetzlicher Änderungen** zu beschließen, mit denen die Möglichkeiten zur Überwachung der Bevölkerung ausgebaut und die Freiheitsrechte weiter eingeschränkt wurden. Dies gilt insbesondere für das Fernmelde- beziehungsweise Telekommunikationsgeheimnis und für das Recht auf informationelle Selbstbestimmung, also für den Datenschutz. Mehr noch als in die Rechte deutscher Staatsangehöriger kann zudem in die Rechte von Ausländerinnen und Ausländern eingegriffen werden.

Fast ausschließlich handelt es sich allerdings bei den gesetzlich beschlossenen erweiterten Befugnissen von Nachrichtendiensten und Polizei um Maßnahmen, die schon früher immer wieder zur Diskussion gestellt worden waren, aber angesichts ihrer Eingriffsintensität in die Grundrechte rechtspolitisch nicht durchsetzbar waren. An einem speziellen Bezug zur Terrorismusbekämpfung fehlt es denn folglich auch oft. Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im Vorfeld der gesetzlichen Beschlussfassung in ihrer Entschließung vom 25. 26. Oktober 2001 (Abdruck im Anhang, Nr. 8) deutlich kritisiert, dass ohne Rücksicht auf das grundrechtliche Übermaßverbot alles vorgeschlagen wird, was technisch möglich erscheint, anstatt zu prüfen, was zur Terrorismusbekämpfung wirklich geeignet und erforderlich ist. Sie haben ebenfalls eindringlich davor gewarnt, dass ein einseitiges Streben nach einer umfassenden Sicherheit nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher **Freiheits- und Persönlichkeitsrechte** so überlagern darf, dass es in unserem Land zu einer lang wirkenden Verschiebung zugunsten staatlicher Überwachung und

zulasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Mittlerweile haben unter anderem der Verfassungsschutz auf Bundes- und Landesebene, der Bundesnachrichtendienst, der militärische Abschirmdienst, Polizei und Strafverfolgungsbehörden **umfassende neue Befugnisse** erhalten. Ohne hier auf Einzelheiten der Unterschiede einzugehen, welche Stelle unter jeweils welchen Voraussetzungen eine Maßnahme durchführen kann, stehen beispielsweise folgende Möglichkeiten zur Verfügung: Die Nachrichtendienste können Daten abfragen und Auskünfte einholen bei Kreditinstituten, bei Luftverkehrsunternehmen sowie bei Unternehmen, die Post- und Telekommunikationsdienste anbieten. Auskünfte über Verbindungsdaten können ebenso verlangt werden wie Auskünfte über die Nutzung von Telediensten. Die Überwachungsmöglichkeiten von Kommunikationsinhalten sind für die Strafverfolgungsbehörden mit Änderungen der Strafprozessordnung erweitert worden. Und nicht zuletzt steht - unter jeweils unterschiedlichen Zulässigkeitsvoraussetzungen - unter anderem den Verfassungsschutz- und Strafverfolgungsbehörden der **IMSI-Catcher** zur Verfügung. Dieses technische Instrument kann Gerätekennung und Kartennummer aktiv geschalteter Handys ermitteln und bezieht dabei sämtliche Handys ein, die sich in seiner Reichweite befinden. Insbesondere wegen dieser Erfassung einer Vielzahl unverdächtiger Personen haben Datenschützerinnen und Datenschützer den Einsatz dieses Gerätes immer abgelehnt.

Ob mit den neuen Gesetzen das Gleichgewicht zwischen Freiheit und Sicherheit nicht nur weiter empfindlich gestört, sondern dauerhaft zu einem Ungleichgewicht verschoben worden ist, hängt auch davon ab, wie in der Praxis mit den neuen Befugnissen umgegangen wird. Daher sollen sie teilweise nach fünf Jahren, also 2007, einer Überprüfung unterzogen werden.

Immer noch nicht vorgelegt wurde die seit längerer Zeit angekündigte Untersuchung der Effektivität derjenigen Telefonüberwachungsmaßnahmen, die nach der Strafprozessordnung richterlich angeordnet werden. Mehr als besorgniserregend ist jedenfalls die wachsende Zahl solcher **Telefonüberwachungen**. Zwar war 2000 in Nordrhein-Westfalen zunächst ein Rückgang derjenigen Verfahren, in denen Anordnungen getroffen wurden, auf 402 (gegenüber 428 in 1999) mit 961 gezielt betroffenen Personen (gegenüber 1208 in 1999) zu verzeichnen. Jedoch wurden 2001 mit 475 Verfahren wieder deutlich mehr Überwachungsmaßnahmen

getroffen, von denen 1101 Personen erfasst wurden, gegen die sich die Maßnahmen gezielt richteten. Darüber hinaus an der Kommunikation beteiligte Personen, gegen die sich die jeweilige Anordnung nicht gezielt richtet, werden unverändert nicht als Betroffene verstanden, obwohl auch in ihre Grundrechte eingegriffen wird.

Für das Ansteigen der Zahlen ist sicherlich auch ursächlich, dass die Verfahren nach dem Betäubungsmittelgesetz insgesamt zunehmen und dies der Bereich ist, in dem mit 325 von 475 Verfahren der Hauptanteil der Telefonüberwachungen stattfindet. Gleichwohl bestätigt dies den Trend, dass sich die Telefonüberwachung von einer ursprünglich als Ausnahme gedachten Maßnahme offensichtlich zu einer Standardmethode bei bestimmten Verfahren entwickelt. Dass auch in 2001 - wie in den Jahren zuvor - keine Telefonüberwachung zu verzeichnen ist in der Rubrik „Anstiftung oder Beihilfe zur Fahnenflucht oder Anstiftung zum Ungehorsam" ist beruhigend. Es zeigt aber auch, wie notwendig es ist, den **Katalog der Straftaten**, bei denen Überwachungsmaßnahmen angeordnet werden können, einmal zu **entrümpeln** statt ihn immer nur zu erweitern. Welche Straftaten gegen die öffentliche Ordnung in neun Verfahren 2001 zu Telefonüberwachungen führten, wäre außerdem von großem Interesse.

Ein Rechtsstaat begegnet seinen Bürgerinnen und Bürgern zunächst einmal mit dem Vertrauen, dass sie sich rechtstreu verhalten. Für staatliche Ermittlungen braucht es demzufolge grundsätzlich zumindest einen Verdacht unrechtmäßigen Handelns. Dieses Grundverständnis hat sich in den letzten Jahren bundesweit schleichend geändert. Schleierfahndung, Videoüberwachung, Rasterfahndung sind nicht zuletzt einige Beispiele dafür. Gerade die nach dem 11. September 2001 - soweit bekannt erfolglos - durchgeführte **Rasterfahndung** muss Anlass dazu geben, über ihre Abschaffung nachzudenken anstatt darüber, die Schwellen für ihren Einsatz auch noch zu senken - wie es in Nordrhein-Westfalen aber leider zu befürchten steht. Angesichts der immer mit einer Rasterfahndung zwangsläufig verbundenen, massenhaft stattfindenden Grundrechtseingriffe, ihrer generell zweifelhaften Erfolgsaussichten und des mit ihr einhergehenden enormen Personal- und Kostenaufwands ist der klassischen polizeilichen Tätigkeit immer der Vorrang einzuräumen.

Mit diesem gewandelten Grundverständnis gelten - zugespitzt formuliert - die Bürgerinnen und Bürger nicht mehr als unverdächtig, sondern nur noch als noch nicht verdächtig. In eine solche Richtung weisen auch weitere Überlegungen, die derzeit auf europäischer, aber auch auf nationaler Ebene

angestellt werden und den Schutz des Telekommunikationsgeheimnisses wie den Datenschutz insgesamt im Bereich der Telekommunikation und der Internetnutzung grundlegend in Frage stellen. Geplant ist, alle diejenigen, die Telekommunikations- und Multimediadienste anbieten, 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 eigenen Geschäftszwecke nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen.

Dabei ist zu bedenken, dass immer mehr menschliche Lebensäußerungen heute in elektronischen Netzen stattfinden. Sie würden bei einer Verwirklichung dieser Pläne einem ungleich höheren **Überwachungsdruck** ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss keine Person bei der Aufgabe eines Briefes im Postamt ihren Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite sie in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitiäten (E-Mail-Versand, Nutzung des World Wide Web) wäre ebenso wenig hinnehmbar. Eine verdachtslose routinemäßige Speicherung auf Vorrat von sämtlichen Daten, die bei der Nutzung von Kommunikationsnetzen anfallen, ist mit dem deutschen Verfassungsrecht nicht zu vereinbaren.

Eine **Kultur des Misstrauens** findet auch im nicht-öffentlichen Bereich zunehmend Verbreitung mit der Folge ständig neuen Datenhungers. Vermögen die Menschen ihrer Menschenkenntnis bei einem Vertragsschluss nicht mehr zu vertrauen, helfen sie sich mit Zusatzinformationen wie vermeintlich objektiven Tatsachenangaben. So sprießen im Internet so genannte **Warndateien** wie Pilze aus dem Boden. Heikel ist dies insbesondere, wenn es um Wohnraum geht, denn eine Wohnung gehört zu den Grundbedürfnissen menschlicher Existenz. Die Datei, mit der Vermieterinnen und Vermieter sich gegenseitig über insolvente oder auf andere Weise vermeintlich unzuverlässige Mieterinnen und Mieter informieren wollen, stieß daher in der Öffentlichkeit moralisch zu Recht auf Protest. Die derzeit geltende Gesetzeslage erlaubt solche Dateien nur in Ausnahmefällen und nur in gewissen Grenzen. Die berechtigte Empörung müsste in der Forderung an den Bundesgesetzgeber münden, die Unzulässigkeit solcher Mieterwarndateien eindeutig und unmissverständlich

zu regeln. Eine nordrhein-westfälische Bundesratsinitiative zu diesem Thema wäre hilfreich.

„Kundenbewertung" nimmt aber nicht nur auf dem Wohnungsmarkt zu, sondern auch in anderen Zusammenhängen und in noch wesentlich systematischerer Form. Immer größeren Absatz findet beispielsweise so genannte Customer-Relationship-Management-Software (CRM). Dabei handelt es sich um Data-Mining-Anwendungen, die riesige Datenmengen analysieren und statistische, unter Umständen auch personalisierbare Urteile fällen. Diese Technik ist vielseitig einsetzbar: Zur Beschäftigtenkontrolle an der Supermarktkasse, zum Erkennen konsumfreudiger, zahlungskräftiger und damit für das Unternehmen bedeutender Kundinnen und Kunden oder zum Herausfiltern der statistischen Wahrscheinlichkeit einer bestimmten politischen Präferenz. Unter welchen Umständen solche Software eingesetzt werden darf oder nicht, ist im Einzelfall unter anderem insbesondere vom Zweck der Datenverarbeitung und der Art der zu verarbeitenden Daten abhängig, insbesondere ihrer Zuordnung zu natürlichen Personen.

Nach der Bundestagswahl 2002 wurde bekannt, dass sich eine politische Partei von der Meldebehörde einer Stadt die Adressdaten aller Wahlberechtigten hatte geben lassen. Sie hatte diese Daten von einer privaten Firma in einer Weise mit statistisch aufbereiteten Daten anreichern und verknüpfen lassen, dass der Eindruck entstand, das Wahlverhalten der namentlich genannten Personen einschätzen zu können. Schon das Vorgehen der Stadt war förmlich zu beanstanden, da das nordrhein-westfälische Melderecht eine Übermittlung der Daten sämtlicher Wahlberechtigten nicht zulässt, sondern nur einzelne, nach dem Lebensalter bestimmte Gruppenauskünfte. Die somit rechtswidrig erlangten Daten hätten zudem nicht weiterverarbeitet werden dürfen. Nicht nur in der privaten Wirtschaft, auch bei manchen politischen Parteien gibt es Bestrebungen, erlaubte oder unerlaubte Mittel zur Durchleuchtung von Kundinnen und Kunden - hier der potentiellen Wählerschaft - zu nutzen. Könnten die Daten von der Meldebehörde nicht so ohne weiteres, sondern nur nach vorheriger **Einwilligung** der Betroffenen an die Parteien herausgegeben werden, wäre schon ein gutes Stück Selbstbestimmung für die Bürgerinnen und Bürger zurückgewonnen. Hier ist der Landesgesetzgeber gefragt!

2 Medien

2.1 Entwicklung des medienrechtlichen Rahmens

Da es nötig war, europarechtliche Anforderungen (im Wesentlichen: eCommerce-Richtlinie RL 2000/31/EG, Signaturrichtlinie RL 1999/93/EG) in nationales Recht umzusetzen, wurden schwerpunktmäßig das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG), der Mediendienstestaatsvertrag (MDStV) und das Signaturgesetz (SigG) geändert. Dabei wurde der Datenschutz nur in Teilen zufriedenstellend berücksichtigt.

Die Änderungen im Bereich der Tele- und Mediendienste betreffen im Wesentlichen die Einführung des Herkunftslandprinzips, die Erweiterung und Präzisierung der Informationspflichten, die Anbieterinnen und Anbieter von Tele- und Mediendiensten zu erfüllen haben sowie ihre Verantwortlichkeit für eigene und fremde Inhalte. **Anonyme** und **pseudonyme Nutzungsmöglichkeiten** sind nach wie vor anzubieten. Auch gilt weiterhin der Grundsatz der **Datenvermeidung**. Diese datenschutzrechtliche Grundsatzforderung ist im Rahmen der Novelle des Bundesdatenschutzgesetzes 2001 in das BDSG aufgenommen worden. Daher wurde auf ihre ausdrückliche Wiederholung im Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag verzichtet. Zu beachten ist sie gleichwohl auch hier. Der Erstellung von **Nutzungsprofilen**, die ohnehin nur zu bestimmten Zwecken und nur unter Verwendung von Pseudonymen zulässig ist, kann nunmehr **widersprochen werden**. Dies stärkt die Rechte der Nutzerinnen und Nutzer. Wie schon in der Telekommunikations-Datenschutzverordnung (TDSV), die das herkömmliche Telefonieren erfasst, wurde nun leider auch im Bereich der Tele- und Mediendienste die **Speicherfrist** für Abrechnungsdaten von früher 80 Tagen auf jetzt 6 Monate heraufgesetzt.

Zugegeben: Das wohl fast ausschließlich der Kompetenzverteilung unter Bund und Ländern geschuldete Nebeneinander von Teledienste- und Teledienstedatenschutzgesetz einerseits und Mediendienstestaatsvertrag andererseits ist nicht glücklich. Es hat von Anfang an rechtliche Unsicherheiten gegeben bei der Zuordnung bestimmter Dienste zu der einen oder der anderen Kategorie. Erst recht streitig ist in der Praxis häufig die Frage, ob ein bestimmter Dienst dem Bereich des Tele- und Mediendiensterechts oder dem Telekommunikationsrecht unterliegt. Die

sich immer stärker entwickelnde **Konvergenz der Medien** erfordert auch einheitliche Anforderungen und Beurteilungsmaßstäbe, um den Datenschutz auf möglichst hohem Niveau gewährleisten zu können. So sinnvoll es sein kann, hier klarere, noch stärker miteinander harmonisierende Regelungen zu schaffen, so alarmierend sind einige der Ideen, die dafür zurzeit in die Diskussion gebracht werden. Nur beispielhaft sei hier die Überlegung genannt, die private Wirtschaft im Endeffekt von (fast) jeder staatlichen Aufsicht im Datenschutz bei elektronischen Medien freizustellen und einer Selbstkontrolle zu überlassen. Dafür ist kein Anlass gegeben. Vielmehr dürfte dieser Ansatz dem Vertrauen in eine wirklich unabhängige und neutrale Datenschutzaufsicht kaum förderlich sein.

Die Datensicherheit im Netz wird durch **elektronische Signaturen** wesentlich gefördert. Sie ermöglichen beispielsweise die eindeutige Zuordnung einer Nachricht zu ihrer Absenderin oder ihrem Absender und das Erkennen, ob eine Nachricht unversehrt und vollständig oder verändert worden ist. Voraussetzung dafür ist eine Sicherungsinfrastruktur. Ihre Ausgestaltung - also etwa die Bedingungen, unter denen Zertifizierungsstellen für die Schlüsselzuordnung genehmigt werden können - ist Gegenstand des **Signaturgesetzes** und der **Signaturverordnung**. Beide Regelungswerke sind im Berichtszeitraum geändert worden, unter anderem aufgrund der Anpassungsnotwendigkeit an europäische Vorgaben.

Auch hier hat die Umsetzung der EG-Richtlinien nicht zur Stärkung des nationalen Datenschutzrechts geführt. Denn nunmehr gibt es auf der unteren Ebene sonstige oder fortgeschrittene Signaturverfahren mit geringeren technischen Auflagen, die keine zentralen Trustcenter zur Verwaltung der Signaturen benötigen, und auf der oberen Ebene die „qualifizierten" Signaturverfahren unter Einbindung von Trustcentern, wobei es sich in der sichersten Ausprägung um ein akkreditiertes Trustcenter handelt. Das frühere Signaturgesetz setzte dagegen ausschließlich auf den höheren Sicherheitsstandard der digitalen Signatur als Siegel mit einer Zertifizierung der Schlüssel durch zugelassene Zertifizierungsstellen. Auf die Beteiligung einer Zertifizierungsstelle wird nunmehr bei der sonstigen und fortgeschrittenen Signatur zum Nachteil der Datensicherheit verzichtet.

Um auch bei der elektronischen Kommunikation rechtsverbindliche Willenserklärungen in denjenigen Fällen abgeben zu können, in denen früher allein die Schriftform vorgesehen war, sind mit dem Gesetz zur Anpassung der **Formvorschriften des Privatrechts** und anderer Vorschriften an den modernen Rechtsverkehr im Juli 2001 die Umstände

geregelt worden, unter denen die Schriftform durch die elektronische Form ersetzt werden kann. Ebenfalls wurde das **Verwaltungsverfahrensrecht** bundesgesetzlich geändert, damit auch im öffentlichen Bereich Dokumente elektronisch übermittelt und Verwaltungsakte elektronisch erlassen werden können. Den datenschutzrechtlichen Bedenken wurde dabei leider nicht hinreichend Rechnung getragen. So wurde beispielsweise nicht die Möglichkeit eröffnet, eine Signatur unter einem Pseudonym zu nutzen. Werden Verwaltungsakte elektronisch erlassen, gelten sie außerdem drei Tage nach ihrer Absendung online als bekannt gegeben. Hier wäre mindestens zuvor die Einwilligung der betroffenen Person einzuholen, den Verwaltungsakt auf elektronischem Wege erhalten zu wollen. Nicht einmal ein Quittungsverfahren zur Absicherung des Postzugangs wurde vorgesehen. Es wäre zu begrüßen, wenn der Landesgesetzgeber seinen Spielraum bei der Umsetzung der bundesrechtlichen Vorgaben in das Landesrecht nutzen würde. Zumindest sollten von der Landesregierung Verwaltungsvorschriften für ein datenschutzgerechteres eGovernment erlassen werden.

2.2 eGovernment: Nur mit Datenschutz ein Serviceangebot an Bürgerin und Bürger

Der Begriff „eGovernment" umfasst die Bemühungen der öffentlichen Verwaltung, ihre Aufgaben mittels der modernen Informations- und Kommunikationstechnologie und insbesondere des Internet zu erfüllen. Hierdurch entstehen für die Nutzerinnen und Nutzer eine Reihe von Risiken und Gefahren für ihr informationelles Selbstbestimmungsrecht, die bei allen Bestrebungen zur Schaffung eines reibungslosen Verwaltungsablaufs berücksichtigt werden müssen.

Mit den Möglichkeiten interaktiver Verwaltung haben sich bereits der 14. Datenschutzbericht 1999 (unter 2.4.3.6 und 2.4.3.7, S. 40 ff), der 15. Datenschutzbericht 2001 (unter 2., insbesondere 2.1.4.3, S. 26) und speziell die Broschüre „Vom Bürgerbüro zum Internet" aus dem Jahr 2000 beschäftigt. Durch eGovernment begibt sich die Verwaltung in zunehmendem Maße in die Abhängigkeit von elektronischen Datenverarbeitungssystemen. Bereits durch die Nutzung der elektronischen Datenübertragung entstehen zusätzliche Risiken der unbemerkten Veränderung und Verfälschung der Daten. Für die Revisionssicherheit sind Protokolle der Nutzungsvorgänge von entscheidender Bedeutung, womit gleichzeitig verstärkt Nutzungsprofile in den Fokus der Betrachtung

gelangen. Vor dem Hintergrund der fortschreitenden Informationsbündelung ist insbesondere die **informationelle Gewaltenteilung** zu gewährleisten - bei gleichzeitiger Einhaltung von rechtlichen, technischen und organisatorischen Standards. Die Menge personenbeziehbarer Daten vervielfacht sich notwendig durch die elektronischen Medien. Gleichzeitig nimmt die Zahl der automatisierten Einzelentscheidungen zu, die ein verstärktes Risiko für die persönlichen Belange und Interessen der Betroffenen mit sich bringen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in Fortführung der Broschüre „Vom Bürgerbüro zum Internet" eine Handreichung „Datenschutzgerechtes eGovernment" erstellt, die unter www.lfd.nrw.de oder in Papierform erhältlich ist.

2.3 Onlineangebote von Kommunen - Nachbesserungsbedarf beim Datenschutz

Im Berichtszeitraum wurden die Internetauftritte von 63 Städten und Gemeinden online kontrolliert. Prüfkriterien waren die sich aus dem Medienrecht ergebenden Verpflichtungen. Bei einigen Kommunen erfolgten Kontrollen „vor Ort", bei denen auch die Sicherheit der Anbindung an das Internet und die hierbei getroffenen technischen und organisatorischen Maßnahmen geprüft wurden.

Bei den Websites der kontrollierten Kommunen war erheblicher Nachbesserungsbedarf in Sachen Datenschutz festzustellen. Die überprüften Inhalte betrafen die Unterrichtungspflicht nach § 4 TDDSG, die Anbieterkennzeichnung nach § 6 TDG, die Notwendigkeit der Verschlüsselung der Übertragung von Formularen (§ 4 Abs. 4 Ziffer 3 TDDSG), Hinweise bezüglich der Weitervermittlung von Informationen an einen anderen Diensteanbieter oder eine andere -anbieterin (Links) gemäß § 4 Abs. 5 TDDSG und schließlich die Anforderung eines Verschlüsselungsangebots bei Übertragungen von E-Mails, hilfsweise den Hinweis auf die Risiken der elektronischen Übertragung mit der Option der Übermittlung per Brief.

Keine der Homepages erfüllte die datenschutzrechtlichen Anforderungen in vollem Umfang. Nur selten wurde § 4 TDDSG vollständig eingehalten und dementsprechend umfassend unterrichtet. Zudem wurde nur in wenigen Fällen eine Verschlüsselung angeboten. Gleiches gilt für den Umgang mit E-Mail-Angeboten. Auch hier fehlte nahezu durchgehend das Angebot einer Verschlüsselung. Kaum eine der betroffenen Kommunen hatte auf die

Risiken der unverschlüsselten E-Mail hingewiesen. Mangelndes Problembewusstsein bestand auch im Bereich der Information der Bürgerinnen und Bürger im Bereich der Verschlüsselung und der Aufklärung bei der Weiterleitung auf andere Angebote.

Bei den Ortsterminen war insbesondere festzustellen, dass häufig **Sicherheitsvorgaben** für die technische Auslegung des Internetübergangs **fehlten**. Auch die **Dokumentation** und **Regelungen** für die Nutzung und den Betrieb waren nur **lückenhaft** vorhanden.

Nach entsprechenden Hinweisen auf die festgestellten Verstöße sind eine Vielzahl von Ergänzungen und Abänderungen durchgeführt worden. Vereinzelt wurden auch Angebote vollständig vom Netz genommen. In Teilen sind die Ergänzungen und Korrekturen noch nicht abgeschlossen, was häufig durch Abstimmungsnotwendigkeiten mit angeschlossenen Rechenzentren bedingt ist.

Insgesamt ist jedoch eine zunehmende Sensibilität für den Datenschutz zu verzeichnen.

2.4 Neue Regelungen zur Überwachung

2.4.1 Der Staat hört mit - Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung (TKÜV) vom 22. Januar 2002 ist seit dem 29. Januar 2002 in Kraft. Hauptkritikpunkt ist, dass sie über das zulässige Maß der Beobachtung von Kommunikation weit hinaus schießt.

In den letzten zwei Berichtszeiträumen wurde immer wieder der Stand der Diskussion über die TKÜV vorgestellt. Gemäß § 88 TKG in Verbindung mit § 3 Abs. 1 TKÜV wird nunmehr eine technische Infrastruktur geschaffen, die eine umfassende Überwachung in offenen Informations- und Kommunikationsnetzen möglich macht. Durch die technikneutrale Definition der Telekommunikation ist der Kreis der Verpflichteten sehr weit gefasst. Zum Kreis der Verpflichteten gehören nach dem Wortlaut der TKÜV auch Internetprovider, die E-Mail- Dienste anbieten. Die TKÜV lässt jedoch Ausnahmen von der Verpflichtung zur Vorhaltung von Überwachungsmaßnahmen für Betreiberinnen und Betreiber von unternehmensinternen Telekommunikationsanlagen, Corporate Networks

und Nebenstellenanlagen, wie sie zum Beispiel in Krankenhäusern oder Hotels betrieben werden, zu.

Das Internet ist ein **Massenkommunikationsmittel** geworden, das immer mehr auch für Alltagsgeschäfte genutzt wird. Es muss der staatlichen Überwachung grundsätzlich entzogen bleiben, da der Internet-Verkehr einen erheblich größeren Teil menschlichen Lebens abbildet als die herkömmlichen Telefongespräche. Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit ihrer Entschließung vom 10. Mai 2001 (Abdruck im Anhang, Nr. 5) gegen die Schaffung einer technischen Infrastruktur gewandt, die es ermöglicht, den Internet-Verkehr umfassend zu überwachen, und damit diesen unverhältnismäßigen Eingriff in das **Grundrecht auf freie Telekommunikation** kritisiert. Zu kritisieren ist auch, dass die Effektivität der bisherigen Überwachungsmaßnahmen nicht vor der Schaffung neuer Eingriffsmöglichkeiten untersucht worden ist. Bis heute liegen keine gesicherten Erkenntnisse vor, ob die Überwachung des Fernmeldeverkehrs tatsächlich zu den gewünschten Ermittlungserfolgen geführt hat. Da die Abhörmaßnahmen stetig angestiegen sind, hat der Gesetzgeber sicher zu stellen, dass Telekommunikationsüberwachungen wegen ihrer hohen Eingriffsintensität nur durchgeführt werden, wenn sie unvermeidbar sind und nicht zum „Standard" von Ermittlungsmaßnahmen werden. Dies leistet die TKÜV nicht. Trotz massiver Vorbehalte und Kritik der Wirtschaft sowie der Datenschutzbeauftragten des Bundes und der Länder wurde die TKÜV verabschiedet.

Kaum in Kraft getreten erfuhr die TKÜV am 16. August 2002 ihre erste Änderung. Sie wurde um Maßnahmen nach den §§ 5 und 8 G 10 - Gesetz ergänzt. Möglich ist jetzt ebenfalls eine strategische Überwachung durch den Bundesnachrichtendienst (BND). Die Verpflichteten haben nun auch für die Maßnahmen des G 10 - Gesetzes Schnittstellen vorzuhalten, da seit dessen Novellierung ebenfalls die leitungsgebundene Telekommunikation in die strategische Überwachung einbezogen ist. Vorher konnte nur die Kommunikation per Satellit überwacht werden. Der Bundesnachrichtendienst kann verdachtslos und ungezielt einen größeren Anteil der Telekommunikation zwischen Deutschland und dem Ausland abhören. Wie allerdings im leitungsgebundenen Verkehr ausgeschlossen werden soll, dass nicht auch die deutschlandinterne Kommunikation überwacht wird, ist eine noch offene Frage.

Aufgrund unterschiedlicher Regelungen und der Schaffung immer neuer Befugnisnormen weitet sich der Gesamtumfang der Telekommunikationsüber-

wachung stetig aus. Dieser Entwicklung muss mit Entschiedenheit entgegen getreten werden.

2.4.2 Cyber Crime Convention - Kriminalitätsbekämpfung um jeden Preis?

Die 44 Mitgliedsstaaten des Europarates und weitere Staaten wie die USA, Kanada, Japan und Südafrika haben gemeinsame Regeln zur Bekämpfung und Verfolgung der Computerkriminalität aufgestellt. Ziel der Cyber Crime Convention ist es, Gesetze und Vorgehensweisen zur Bekämpfung verschiedener Arten kriminellen Verhaltens gegen Computer-Systeme, -Netzwerke und -Daten bereitzustellen.

Der Europarat hat am 08. November 2001 in Budapest die Cyber Crime Convention zur Bekämpfung von Computerkriminalität verabschiedet. Die ersten Staaten haben das Regelwerk am 23. November 2001 unterzeichnet, mit dabei auch Deutschland. In der Cyber Crime Convention werden Vergehen definiert, die mit Hilfe des Internet verübt werden können. Sie **erweitert die Befugnisse für das Abhören** der Internetkommunikation und enthält Regelungen zum grenzüberschreitenden Verfahren und zum Datenaustausch zwischen den Strafverfolgungsbehörden. Die Cyber Crime Convention ermöglicht die Speicherung vorhandener Computerdaten, wie zum Beispiel von Geschäfts-, Kranken-, Personal- oder anderen Unterlagen und Verbindungsdaten der Telekommunikation sowie deren Herausgabe und Beschlagnahme und schließlich die Durchsuchung von Computersystemen. Auch das Mitschneiden von Verbindungsdaten und Inhaltsdaten der Telekommunikation und des Internet wird geregelt. Es werden den Providern Speicherfristen für sämtliche Daten von bis zu 90 Tagen vorgeschrieben.

Kernproblem der Cyber Crime Convention ist das **unausgewogene Verhältnis** zwischen der Bekämpfung von Computerkriminalität und den Freiheits- und Datenschutzrechten der überwiegenden Anzahl rechtstreuer Internetnutzerinnen und Internetnutzer. Es gibt so gut wie keine Regelungen für den Umgang mit personenbezogenen Daten oder dem Fernmeldegeheimnis, geschweige denn Regelungen über den Umgang mit den Daten, die aufgrund von Amtshilfe durch Drittstaaten erlangt wurden, deren Datenschutzniveaus wesentlich schlechter ist als das der Staaten der europäischen Union. Die Überwachung der Individualkommunikation muss

eine Ausnahme bleiben, da es ansonsten zu einer Aushöhlung des Rechts auf unbeobachtete Kommunikation kommt.

Bei der Umsetzung der Cyber Crime Convention in nationales Recht müssen der Datenschutz und das Fernmeldegeheimnis gewährleistet bleiben. Grundrechtseingriffe sind auf das unabdingbare Maß zu begrenzen. Der Zugriff und die Nutzung von personenbezogenen Daten sind einer strikten und eindeutigen Zweckbindung zu unterwerfen. Es ist auch dafür Sorge zu tragen, dass die Daten von Internet-Nutzenden nur in Länder übermittelt werden, in denen ein angemessenes Datenschutzniveau herrscht. Dies hat auch die 61. Datenschutzkonferenz des Bundes und der Länder am 08./09. März 2001 gefordert (Abdruck im Anhang, Nr. 2).

2.4.3 Protokollierung der Daten bei den Providern

Die gesetzlichen Vorgaben für die Protokollierung und Speicherung der anfallenden Datenströme bei Internetprovidern sind im Teledienstedatenschutzgesetz (TDDSG) und im Mediendienstestaatsvertrag (MDStV) geregelt. Dort ist festgelegt, welche Daten erhoben und wie lange sie gespeichert werden dürfen.

Nach § 5 TDDSG und § 19 Abs. 1 MDStV dürfen Bestandsdaten, die für die Begründung und inhaltliche Ausgestaltung von Verträgen erforderlich sind, gespeichert werden. Nutzungsdaten nach § 6 TDDSG und § 19 Abs. 2 MDStV dürfen nur dann über das Ende des Nutzungsvorganges hinaus gespeichert werden, wenn sie der Abrechnung dienen. Diese Abrechnungsdaten dürfen höchstens bis zu sechs Monaten nach Rechnungsstellung oder bei einem Streit über die Rechnung bis zu dessen Klärung gespeichert werden.

Um die gesetzlichen Vorgaben auch zu erfüllen, müssen die Rechtsbegriffe transparent gemacht werden, das heißt, die Fülle der beim Surfen im Internet anfallenden Daten muss den verschiedenen Datenarten zugeordnet werden. **Bestandsdaten** und **Abrechnungsdaten** sind hinreichend in den Gesetzen beschrieben, so dass sich kaum Zuordnungsschwierigkeiten ergeben. Anders sieht es bei den Nutzungsdaten aus. Bei der Novellierung des TDDSG und des MDStV ist versucht worden, Nutzungsdaten gesetzlich zu definieren: Nach § 6 Abs. 1 TDDSG und § 19 Abs. 2 MDStV sind **Nutzungsdaten** insbesondere:

a) Merkmale zur Identifikation des Nutzers oder der Nutzerin.

b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und

c) Angaben über die von der Nutzerin oder dem Nutzer in Anspruch genommenen Teledienste.

Bei den im Berichtszeitraum besuchten Accessprovidern und Backboneprovidern werden hauptsächlich folgende Nutzungsdaten mitprotokolliert: Kennung, Telefonnummer, Startzeit plus Modemgeschwindigkeit, IP-Adresse temporär, Speicherung sämtlicher Bewegungen und Adressen im Internet, Stoppzeit. Obwohl die IP-Adresse ein Nutzungsdatum ist, das nicht zur Abrechnung benötigt wird, speichern alle besuchten Provider die temporäre IP-Adresse über den Nutzungszeitraum hinaus. Dies stellt einen Verstoß gegen § 6 Abs. 4 TDDSG dar. Die IP-Adresse ist mit Beendigung der Internetverbindung zu löschen.

Dynamische IP-Adressen sind nach Ende der Nutzung zu löschen. Da sie nicht zur Abrechnung erforderlich sind, dürfen sie auch nicht als Abrechnungsdatum gespeichert werden.

2.4.4 Überwachung wird mobil

Konnte im 14. Datenschutzbericht 1999 unter 2.4.2.3, S. 32, noch davon gesprochen werden, dass die damals geplanten Regelungen zum Einsatz von IMSI-Catchern nicht verabschiedet wurden, gilt nun etwas anderes. Die Nachrichtendienste, also der Verfassungsschutz in Bund und Land, der Militärische Abschirmdienst (MAD), der Bundesnachrichtendienst (BND) und die Strafverfolgungsbehörden haben mittlerweile Rechtsgrundlagen dafür erhalten, diese von Datenschützerinnen und Datenschützern immer abgelehnten Geräte einzusetzen.

Der IMSI-Catcher dient dazu, die auf Mobilfunkkarten gespeicherte Netzkennung (IMSI) sowie die Gerätekennung (IMEI) zu erfassen und den Standort eines aktiv geschalteten mobilen Endgerätes zu ermitteln. In weiteren Schritten können dann auch die Telefonnummern und letztlich die Namen derjenigen Handybesitzerinnen und Handybesitzer herausgefunden werden, die sich in der jeweiligen Funkzelle befinden. In die Überwachung mit dem IMSI-Catcher werden zwangsläufig jeweils eine **Vielzahl unverdächtiger Personen einbezogen**.

Nach § 100i Strafprozessordnung (StPO) ist der Einsatz des Gerätes durch die Strafverfolgungsbehörden in zwei Fällen vorgesehen. Einmal ist er zur

Vorbereitung einer Maßnahme nach § 100a StPO, also zur Überwachung der Telekommunikation einer Person, die einer Katalogstraftat verdächtigt wird, einsetzbar. Daneben kann er zur Vorbereitung der vorläufigen Festnahme oder Ergreifung eines Täters oder einer Täterin aufgrund eines Haftbefehls oder Unterbringungsbefehls bei Straftaten von erheblicher Bedeutung eingesetzt werden. Dabei ist der Begriff „Straftat von erheblicher Bedeutung" ein unbestimmter Rechtsbegriff, der zwar mindestens eine Tat aus dem Bereich der so genannten mittelschweren Kriminalität verlangt, gleichwohl jedoch ein weites Einsatzfeld umfasst. Die Nachrichtendienste dürfen den IMSI-Catcher zur Standortermittlung eines Handys sowie zur Ermittlung der Geräte- und Kartennummern einsetzen. Allerdings **fehlen konkrete Tatbestandsvoraussetzungen**, wie etwa die Festlegung einer bestimmten Verdachtsschwelle und die Beschränkung auf schwerwiegende Gefahren.

Der IMSI-Catcher sollte nicht eingesetzt werden, weil er immer auch eine Vielzahl unverdächtiger Personen erfasst.

2.5 Presse - genügt freiwillige Selbstkontrolle für einen effektiven Datenschutz?

Derzeit liegt ein Gesetzentwurf vor, mit dem die Rahmenvorschrift des § 41 Abs. 1 BDSG in nordrhein-westfälisches Landesrecht umgesetzt werden soll. Geplant ist, auf Grund des § 41 Abs. 1 BDSG den Pressekodex des Deutschen Presserates um Regelungen zum Redaktionsdatenschutz zu ergänzen.

Redaktionen, die Mitgliedsorganisationen des Trägervereins des Deutschen Presserates angehören, sollen im Rahmen der **freiwilligen publizistischen Selbstkontrolle** von sich aus falsche oder unzulässig erhobene Daten über Personen richtig stellen beziehungsweise sperren. Allgemeine Datenschutzrichtlinien im Pressekodex betreffen sowohl Auskunft und Löschung sowie die Dokumentation personenbezogener Daten als auch den Umfang zulässiger Datenübermittlung. Der Presserat soll im Rahmen der freiwilligen publizistischen Selbstkontrolle über Beschwerden zur Erhebung, Speicherung und Veröffentlichung personenbezogener Daten in Redaktionen im eigens dafür eingerichteten unabhängigen Beschwerdeausschuss entscheiden können.

Problematisch ist hier jedoch, dass es keine Pflichtmitgliedschaft von Presseunternehmen beim Deutschen Presserat gibt und die Nichtmitglieder

nicht der publizistischen Selbstkontrolle unterworfen sind. Hinzu kommt, dass die Effektivität der Entscheidungen des geplanten Beschwerdeausschusses zweifelhaft ist. Im Ergebnis ist der EG-Datenschutzrichtlinie damit nicht Genüge getan.

2.6 Einzelfragen zu Telekommunikation, Internet und E-Mail

2.6.1 Aufnahme in elektronische oder gedruckte Telefonverzeichnisse

Viele Bürgerinnen und Bürger beschweren sich darüber, dass sie, obwohl sie dies nicht beantragt haben, in Telefonverzeichnisse aufgenommen wurden. Bei den Beschwerden geht es in Teilen um den Eintrag als Ganzes, aber auch um Falscheinträge oder Einträge in das jeweils falsche Medium wie CD-ROM oder die Gelben Seiten.

Nach dem Telekommunikationsrecht dürfen Telekommunikationsdienste-anbieterinnen und -anbieter nur dann Einträge ins **öffentliche Kundenverzeichnis** aufnehmen, wenn dies ausdrücklich beantragt wurde. Das Telekommunikationsrecht hat sich diesbezüglich in den letzten Jahren zu Gunsten der Kundinnen und Kunden verbessert. Nachdem es zunächst einen Zwangseintrag gab, konnte später einem solchen Eintrag widersprochen werden. Nunmehr können Kundinnen und Kunden selbst entscheiden, ob sie nur in gedruckte oder auch in elektronische Verzeichnisse aufgenommen werden wollen und welche Angaben, beispielsweise Name, Anschrift, Beruf, Branche überhaupt in diesen Verzeichnissen veröffentlicht werden sollen. Der Wunsch nach Löschung oder Änderung dieser Angaben muss schnellstmöglich umgesetzt werden. Bei der Antragstellung sollte Klarheit darüber bestehen, dass die **Rufnummer weltweit über Online-Dienste** zur Verfügung steht und auch in diversen **CD-ROM-Verzeichnissen**, im Ausland sogar mit der Möglichkeit der **Rückwärtssuche**, über den Handel vertrieben wird. Rückwärtssuche bedeutet in diesem Zusammenhang, dass nach Eingabe einer Rufnummer Name und Anschrift der betreffenden Person ermittelt werden. Nach deutschem Recht ist dies gem. § 14 Abs. 5 TDSV nicht zulässig. Ein Anspruch auf Löschung der Daten bei bereits im Handel erhältlichen Versionen besteht allerdings nicht.

Fehler bei Anträgen oder Änderungen können sowohl bei den jeweiligen Telekommunikationsunternehmen als auch bei den Verlagen der Druck- und

CD-ROM-Verzeichnisse liegen. Soweit Fehler bei der Erhebung der Daten durch die Telekommunikationsunternehmen liegen, werden die Beschwerden an die gemäß § 91 Abs. 4 TKG zuständige Kontrollinstanz abgegeben. Das ist der Bundesbeauftragte für den Datenschutz in Bonn. Liegt die Fehlerursache jedoch bei den Verlagen der Druck- oder CD-ROM-Verzeichnisse, weil zum Beispiel gesetzte Sperrvermerke nicht berücksichtigt wurden, so handelt es sich um einen Verstoß gegen § 29 Abs. 3 BDSG. Erfahrungsgemäß ist die Ursache jedoch bei den Telekommunikationsunternehmen zu suchen, da die Eingabe der Kundinnen- und Kundendaten und -wünsche meistens manuell erfolgt. Das Auslesen der Sperrvermerke läuft dagegen regelmäßig in automatisierten Verfahren, so dass hier Fehler eher selten sind.

2.6.2 Spamming und Newsletter

Anlass vieler Beschwerden sind das Spamming (E-Mail-Werbung) und die Zusendung von Newslettern. Dabei wird in der Hauptsache nachgefragt, ob es Abwehrmöglichkeiten gibt, wie die Absendenden an die E-Mail-Adresse gelangen und was die Anbietenden an personenbezogenen Daten gespeichert haben.

Der Begriff „**Spam**" geht auf einen Sketch der englischen Komikergruppe „Monthy Python's Flying Circus" zurück, in dem das gleichnamige Dosenfleisch-Produkt eines amerikanischen Herstellers ungefragt zu jedem Gericht serviert wurde. Als Spam werden Rundschreiben mit überflüssigem, teils dubiosem oder werbendem Inhalt verstanden, die mittels E-Mail massenhaft an eine nicht zielgerichtete Empfängergruppe verschickt werden.

Die Versendung von Spammails ist primär ein Problem des **unlauteren Wettbewerbs**. Erst wenn die Empfängerinnen und Empfänger solcher Mails den Absenderinnen und Absendern die Nutzung ihrer Daten untersagen und die Löschung oder Sperrung dieser Daten verlangen, kann gegebenenfalls ein Verstoß gegen Datenschutzbestimmungen vorliegen. Ein Auskunftsbegehren, wie es von den Betroffenen gegenüber den Absenderinnen und Absendern oft verlangt wird, über den Umfang der zu ihrer Person gespeicherten Daten und deren Herkunft führt häufig nicht zum gewünschten Ergebnis, da diesen Unternehmen in der Regel nur die E-Mail-Adressen vorliegen und diese aus dem Internet heraus gescannt wurden. Da Unterlassungs- oder Schadensersatzklagen nur kostspielig und zeitintensiv

sind und die Absender, insbesondere von Erotik-Spams, oft nur schwer zu ermitteln sind, sind folgende **Handlungsempfehlungen** zu beachten:

Bei der Bekanntgabe der E-Mail-Adresse gegenüber Dritten ist Vorsicht walten zu lassen und ein gewisses Fingerspitzengefühl dafür zu entwickeln, wem die eigene E-Mail-Adresse mitgeteilt werden kann. Es empfiehlt sich außerdem - soweit dies möglich ist - die eigene E-Mail-Adresse nicht in E-Mail-Verzeichnisse im Internet einzutragen, um sich wenigstens teilweise vor Spamming zu schützen. Einen weiteren und effektiven Schutz bieten so genannte **E-Mail-Filter**. Dabei handelt es sich um Programme, die dafür sorgen, dass nur solche E-Mails empfangen werden können, die für den Empfang freigegeben wurden. Unter Umständen bieten auch Provider die Möglichkeit an, einzelne E-Mail-Adressen, über die bereits Spam versandt wurde, in eine so genannte „Anti-Spam-Liste" einzutragen. Von diesen Adressen ausgehende Mails werden dann zukünftig blockiert und gelangen nicht mehr in den Posteingang der Nutzenden.

Newsletter sind eine Sonderform von Mailing-Listen. Es handelt sich um einen E-Mail-Verteiler, bei dem lediglich Informationen (News) an bestimmte Zieladressen verteilt werden. Newsletter informieren über ein bestimmtes Thema, ohne ein Diskussionsforum zu bieten. Inzwischen werden sie in der Hauptsache als Marketinginstrument, für Pressemitteilungen und zum Zwecke der Kundenbindung eingesetzt.

Aus datenschutzrechtlicher Sicht problematisch ist der Umfang der geforderten **Registrierungsangaben** und die meist **fehlende Unterrichtung** über den Umgang mit personenbezogenen Daten. Bei der Gestaltung dieses Angebotes sind die Vorschriften des TDG und TDDSG zu beachten. Daraus folgt, dass Diensteanbieterinnen und Diensteanbieter gemäß § 4 Abs. 1 TDDSG die Nutzerinnen und Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten haben. Hierzu gehören auch Informationen darüber, welche Daten über welchen Zeitraum erhoben und gespeichert werden und ob gegebenenfalls Daten für andere Zwecke verwendet oder an Dritte übermittelt werden. Bei den meisten Angeboten von Newslettern genügt die Angabe einer gültigen E-Mail-Adresse, einige wenige jedoch verlangen darüber hinaus gehende Angaben, beispielsweise Name, Anschrift, Geburtsdatum, Hobbys und Ähnliches. Dies ist ein Verstoß gegen § 4 Abs. 6 und § 5 TDDSG und somit unzulässig, weil diese Angaben für die Erbringung dieses Dienstes nicht erforderlich sind. Zusätzliche Angaben dürfen nur auf freiwilliger Basis mittels einer

elektronischen Einwilligungserklärung nach § 4 Abs. 2 TDDSG erhoben, verarbeitet und genutzt werden

Zur Vermeidung von Spammails und unerwünschten Newslettern ist in erster Linie auf eine Zurückhaltung bei der Weitergabe der E-Mail-Adresse zu achten. Sie sollte nur an vertrauenswürdige Personen oder Anbietende weitergegeben werden.

2.6.3 Elektronische Formulare

Auf vielen Internetseiten werden elektronische Formulare zur direkten Übertragung von Informationen genutzt. Neben den typischen Registrierungsangaben und gegebenenfalls zusätzlichen freiwilligen Informationen zur Person werden dabei auch freie Felder für Kommentare angeboten. Seitens der Nutzer und Nutzerinnen wird immer wieder die Vertraulichkeit der dort übertragenen Informationen angesprochen.

Der Zweck dieser Formulare ist unterschiedlichster Natur und reicht von einfachen Kontaktaufnahmeformularen bei Unternehmen bis hin zur Online-Beichte. Soweit bei diesen Formularen personenbezogene oder personenbeziehbare Daten übertragen werden, ist neben den Grundsätzen der **Datenvermeidung**, Datensparsamkeit und der vorzunehmenden **Unterrichtung** auch die **Verschlüsselung** zu beachten.

Viele Nutzerinnen und Nutzer kennen das Problem: Daten, die über das Internet unverschlüsselt im Klartext übertragen werden, können weltweit ohne viel Aufwand mitgelesen werden. Aus diesem Grunde hat der Gesetzgeber § 4 Abs. 4 Nr. 3 in das Teledienstedatenschutzgesetz aufgenommen. Danach haben Diensteanbieterinnen und Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste **gegen Kenntnisnahme Dritter geschützt** in Anspruch genommen werden können. Dies bedeutet letztlich, dass dafür Sorge zu tragen ist, dass niemand erfährt, ob und wie Teledienste genutzt werden. Der Schutzbereich umfasst sowohl die Inhaltsdaten als auch die Nutzungs-, Abrechnungs- und Bestandsdaten. Etliche Anbieterinnen und Anbieter scheinen sich dieser Verpflichtung jedoch nicht bewusst zu sein.

Zur Wahrung der Vertraulichkeit im Internet ist der Einsatz entsprechender Authentifizierungsmechanismen und Verschlüsselungstechniken von zentraler Bedeutung. Er erfolgt derzeit allerdings immer noch zu zögerlich.

2.6.4 Internet-Cafés

Internet-Cafés erfreuen sich einer großen Beliebtheit. Vielen Nutzerinnen und Nutzern ist allerdings nicht bewusst, welche Spuren sie hierbei hinterlassen können.

Möchte man einfach nur ein wenig surfen, kann es günstig sein, „mal eben" in ein Internet-Café zu gehen und gegen einen Pauschalpreis eine gewisse Zeit im Internet zu verbringen. Was auch heute viele jedoch noch nicht wissen ist, dass je nach Systemeinstellungen des Rechners und des verwendeten Browsers die Nutzenden viele **Spuren** von und über sich auf dem Rechner **im Café hinterlassen** können. So bieten die gängigsten Browser beispielsweise die Möglichkeit der automatischen Passwortspeicherung. Das bedeutet, dass nachfolgende Nutzer und Nutzerinnen nur die Kennung ihrer Vorgänger und Vorgängerinnen mitlesen brauchen und das System das Passwort automatisch ergänzt. Eine weitere Möglichkeit, etwas über die vorhergehende Nutzung zu erfahren, sind die temporären Internetdateien oder der so genannte Verlauf. Mittels dieser Optionen lässt sich gegebenenfalls genau nachvollziehen, welche Seiten besucht wurden. Bei den temporären Internetdateien können sogar **Kopien der aufgerufenen Mails** gespeichert werden. Noch aussagekräftiger und riskanter wird es, wenn es auf diesen Rechnern gestattet ist, mittels zusätzlicher Programme eigene Dokumente zu erstellen und auf der Festplatte zu speichern oder selbst von einer Diskette zu laden. Neben der Gefahr des **Virenbefalls** und des Einfangens von **Trojanischen Pferden** besteht auch die Gefahr, dass einfach vergessen wird, diese Dateien und oben beschriebenen Spuren zu löschen.

Eine ideale Lösung für die Nutzung von Rechnern in Internet-Cafés besteht in folgendem Vorgehen: Zunächst meldet der Besucher oder die Besucherin sich anonym an und bezahlt die jeweilige Gebühr. Diskettenlaufwerk und Festplattenzugriff werden durch die Administration gesperrt. Der jeweilige Browser wird automatisch gestartet und die Nutzung zusätzlicher Software ausgeschlossen. Die Browsereinstellungen werden derart vorgenommen, dass keine personenbezogenen Daten gespeichert und die temporären Internetdateien sowie die Dokumentation des Sitzungsverlaufs nach Beendigung automatisch gelöscht werden.

2.6.5 Chats und Foren

Bei Chats und Foren liegen die Datenschutzprobleme meist in der Registrierung und der Datenübermittlung an so genannte Operatoren.

Forum ist der Oberbegriff für verschiedene Arten von Onlinediskussionen. Sie bilden den Treffpunkt von Nutzenden mit ähnlichem Interesse. Der Informationsaustausch erfolgt dabei auf verschiedene Arten beispielsweise über **Newsgroups** oder **Chats**. Bei Newsgroups findet in der Regel ein Informationsaustausch zu bestimmten Themen statt. Die Teilnehmenden veröffentlichen hierbei einen Artikel, auf den andere antworten können. Einige Newsgroups werden moderiert, das bedeutet, es findet auch eine Kontrolle der Inhalte statt. Moderatorinnen und Moderatoren können dann darüber entscheiden, ob bestimmte Artikel veröffentlicht werden oder ob ein Forum geschlossen wird. Im Gegensatz dazu handelt es sich bei Chats um eine gleichzeitige weltweite Unterhaltung mit mehreren Teilnehmenden. Die Tastaturunterhaltung der Teilnehmenden erscheint auf den Bildschirmen in der Reihenfolge der Eingabe.

Die Inhalte und die Übermittlung der Inhalte ist datenschutzrechtlich meist unproblematisch, da den Nutzerinnen und Nutzern bewusst ist, dass die Beiträge weltweit gelesen werden können und sie für sich selbst entscheiden können, was sie über die eigene Person offen legen. Die hier eingegangenen Nachfragen beziehen sich zumeist auf den Umfang der Datenerhebung im Zusammenhang mit der **Registrierung** und die **Datenübermittlung an Dritte**: Müssen beispielsweise die eigene E-Mail-Adresse, die reale Postanschrift oder das Geburtsdatum bei der Registrierung angegeben werden? Dürfen Pseudonym und IP-Adresse an Dritte, insbesondere an die Operatoren, weitergegeben werden?

Ob Foren nun als Teledienste oder als Mediendienste zu qualifizieren sind, kann dahingestellt bleiben, da die datenschutzrechtlichen Regelungen inhaltsgleich sind. Zunächst gilt der Grundsatz der **anonymen Nutzung**. Diensteanbieterinnen und -anbieter haben den Nutzenden die Inanspruchnahme der Dienste und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Ohne Einwilligung dürfen **Bestandsdaten**, dies sind beispielsweise Name, Anschrift, E-Mail, Pseudonym oder Passwort, nur erhoben, verarbeitet oder genutzt werden, soweit dies für die Begründung, inhaltliche Ausgestaltung

oder Änderung eines Vertragsverhältnisses erforderlich ist. Die **Erforderlichkeit** ist mit **strengen Maßstäben** zu prüfen.

Die Speicherung des Pseudonyms und des Passworts ist zweifelsfrei zulässig, da sie zur Anmeldung und Nutzung des Dienstes benötigt werden. Darüber hinaus gehende Angaben sollten, wenn überhaupt, nur nach **vorhergehender Unterrichtung** über den Verarbeitungszweck optional erfolgen, um so den Nutzenden die Möglichkeit der faktischen Anonymität zu geben. Ein zwingender Erforderlichkeitsgrund zur Erhebung weiterer Bestandsdaten ist nicht erkennbar.

Nutzungsdaten dürfen ohne Einwilligung der Betroffenen nur erhoben, verarbeitet oder genutzt werden, soweit dies erforderlich ist, um den angebotenen Dienst zu ermöglichen oder abzurechnen. Nutzungsdaten, die keine Abrechnungsdaten sind, sind frühestmöglich zu löschen, spätestens unmittelbar nach Ende der jeweiligen Sitzung.

Da die Nutzung von Foren in der Regel kostenlos erfolgt, dürfen somit bei den Diensteanbieterinnen und Diensteanbietern auch **keine Nutzungsdaten gespeichert** oder genutzt werden. Entsprechendes gilt auch für die Übermittlung der Nutzungsdaten an so genannte Operatoren oder für das Veröffentlichen der jeweiligen Daten im Forum selbst. Da die Übermittlung dieser Daten an Dritte für die Inanspruchnahme des Dienstes nicht erforderlich ist, ist sie unzulässig.

Beim Betrieb von Chats und Foren ist besonders darauf zu achten, dass nur zwingend erforderliche Bestandsdaten gespeichert werden. Nutzungsdaten sind jeweils unmittelbar nach den Sitzungen zu löschen.

3 Technik

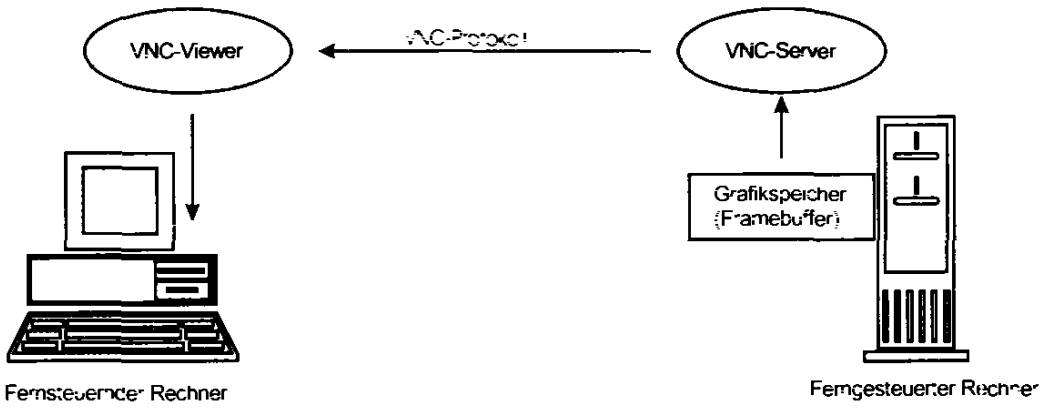
3.1 Ferngesteuerte Internetanbindung

Zu den Gefahren, die in jüngster Zeit zunehmend im Internet lauern, gehören so genannte Spionageprogramme. Dies sind kleine Applikationen, die unbemerkt auf einen Rechner geschmuggelt werden und, einmal aktiv, entweder persönliche Daten an einen Datenspion übermitteln oder einfach nur Schaden auf dem betreffenden Rechner anrichten können. Neben Back Orifice, Netbus oder SubSeven wird auch eine Software namens VNC erwähnt, die in der Lage ist, einen Rechner über das im Internet genutzte TCP/IP-Protokoll fernzusteuern. Datenschutzbeauftragte stehen einer solchen Technik naturgemäß skeptisch gegenüber, doch in diesem Falle hat die Software durch Umkehrung der Übertragungsrichtung eine unter Datensicherheitsaspekten positive Kehrseite.

Die Bezeichnung VNC (Virtual Network Computing) entstand ursprünglich im Olivetti & Oracle Research Laboratory (ORL) im Rahmen der Entwicklung eines Netzwerk-Computers für die Client-Server Architektur, der über minimale Rechenleistung verfügen sollte. Die Grundidee war, die Menge der zwischen Server und Client ausgetauschten Daten zu minimieren. Also wurde eine (sehr kleine) Software entwickelt, die lediglich die reinen Grafikdaten einer Serverapplikation zum Client überträgt. Alle Rechenschritte der jeweiligen Anwendung werden auf dem Server ausgeführt. Die Steuerung der Anwendung erfolgt umgekehrt durch Übertragung von Informationen über Mauszeiger oder Tastatureingaben. Somit ist es möglich, einen beliebig weit entfernten Rechner fernzusteuern, der über ein wie immer geartetes Netzwerk verbunden ist (Internet, LAN, Firewire, USB).

Der betreffende Rechner kann über ein nahezu beliebiges Betriebssystem verfügen und benötigt nicht einmal einen Bildschirm, denn VNC überträgt den Inhalt des so genannten Framebuffers. Dieser ist ein spezieller Speicher für die Informationen über jedes einzelne Pixel (kleinstes darstellbares Rechteck eines Computer-Displays), die ein Rechner benötigt, um einen kompletten Bildschirm darstellen zu können. Der Inhalt wird nun von dem Teil von VNC, der auf dem fernzusteuernden Rechner installiert wurde, dem „VNC-Server", über das VNC-Protokoll auf den fernsteuernden Rechner transportiert und von dem dort installierten „VNC-Viewer" als Fenster dargestellt. Der Bildschirminhalt des ferngesteuerten Rechners ist zu

jeder Zeit identisch mit dem Fensterinhalt des Viewers, so dass simultan mehrere Nutzende solcher Viewer beispielsweise ein Textdokument bearbeiten können.



VNC-Kommunikation

Ursprünglich war das Einsatzgebiet von VNC die Fernwartung von PC, aber auch das widerrechtliche Fernsteuern fremder Rechner über das Internet ist ebenso komfortabel möglich. Deshalb war der Ruf dieser Software ein sehr zweifelhafter. Was hat eine solche Software nun mit Datenschutz zu tun?

Wird die Kommunikation zwischen VNC-Server und -Viewer betrachtet, so ergibt sich bei Umkehr der Rollen ein interessanter Sicherheitsaspekt: Wird ein Rechner mit dem Internet verbunden und auf diesem der VNC-Server installiert, kann über einen zweiten Rechner mittels des VNC-Viewers auf diesen zugegriffen werden, ohne dass Inhalte aus dem Internet direkt auf den mit dem Viewer ausgestatteten Rechner gelangen können. Das VNC-Protokoll überträgt in Richtung des Viewers bekanntlich nur die Inhalte des Grafikspeichers.

So können in der praktischen Anwendung sensible Daten auf einem Rechner gespeichert werden, der (indirekt) mit dem Internet verbunden ist, **ohne** dass die **Gefahr des Ausspähens**, Manipulierens oder auch nur der Kenntnisnahme besteht. Der mit dem Internet verbundene Rechner kann zusätzlich mit allen gängigen Sicherheitsmechanismen geschützt werden, so dass die Gesamtverfügbarkeit des Systems gewahrt bleibt.

Performance, technische Plattform, Restrisiken

Für einen einzelnen Arbeitsplatz ist die VNC-Anbindung an das Internet allerdings zu aufwändig. Die physikalische Trennung von internem und externem System wäre in diesem Fall nicht aufwändiger, aber sicherer.

Ist aber der an das Internet angebundene Rechner multi-user- und multi-taskingfähig, so kann er für eine beliebige Anzahl von Nutzenden virtuelle Bildschirme von beispielsweise Browseranwendungen zur Verfügung stellen. Dies stellt sich den Nutzenden wie eine Terminalemulation dar, die auf ihrem Desktop als Symbol dargestellt und wie eine Anwendung auf dem jeweiligen Rechner bedient werden kann. Durch die hohe Effizienz des VNC-Protokolls ist bei entsprechender Dimensionierung des VNC-Servers die Geschwindigkeitseinbuße gegenüber einer direkten Internetanbindung zu vernachlässigen.

Ein kleiner Wermutstropfen trübt dann zum Schluss die schöne neue Anbindungswelt: Die fehlende Möglichkeit des physikalischen Übertragens von Dateien vom internen in das externe System und umgekehrt. Können externe Downloads oder Attachements aus E-Mails noch mittels VNC auf dem Server zumindest geöffnet und gelesen werden, so ist der Weg vom internen in das externe Netz komplett verschlossen. Das ist unkomfortabel, könnte aber durch das manuelle Überspielen der gescannten Dateien gelöst werden. Ein weiterer Mangel beeinträchtigt jedoch die Vertraulichkeit: Verschlüsselte E-Mails, die nur von einer Person oder einem eingeschränkten Personenkreis gelesen werden dürfen, müssen auf dem Server entschlüsselt werden, damit die Grafikdaten der entschlüsselten E-Mail zum Rechner der berechtigten Person übertragen werden können. Dort besteht grundsätzlich die **Gefahr der Einsichtnahme durch Unberechtigte**. Hier muss ein abgeschotteter Bereich, zum Beispiel ein eigener Entschlüsselungsserver, geschaffen werden, auf dem sichergestellt wird, dass geheime Schlüssel weder kompromittiert noch manipuliert beziehungsweise entschlüsselte Mails unbefugt mitgelesen werden können.

Die Anbindung eines Intranet an das Internet mittels VNC bietet nicht ganz die Sicherheit eines Systems, bei dem externes und internes Netz getrennt betrieben werden, hat demgegenüber aber den Vorteil, dass nicht jeder Arbeitsplatz mit zwei Rechnern ausgestattet werden muss. Das **Problem des sicheren Transports** von Dateien zwischen internem und externem Netz wird von beiden Architekturen noch nicht gelöst.

Wer Interesse an weitergehenden Informationen hat, kann Kontakt mit dem „virtuellen Datenschutzbüro" (www.datenschutz.de) aufnehmen, einem gemeinsamen Service verschiedener nationaler und internationaler Datenschutzinstitutionen, bei dem diese Art der Anbindung seit längerem im Praxisbetrieb erfolgreich erprobt wird.

3.2 Biometrie - ein Allheilmittel zur Identifikation?

Selbst große IT-Muffel kommen heute nicht mehr umhin, sich eine Reihe von Passworten oder PIN-Codes für die Nutzung der sie umgebenden technischen Systeme zu merken. Handys, Kreditkarten, PCs, Zugangskontrollsysteme, Internetaccess - um einige zu nennen - erfordern in der Regel zum Nachweis der Berechtigung die Angabe von Passworten. Werden bei der Ausprägung die allgemein anerkannten Grundsätze für die Struktur, Länge und Änderung von Passworten zugrunde gelegt, wird deutlich, dass es ohne Hilfsmittel, inhaltliche Brücken oder Vereinfachungen häufig nicht möglich ist, sich Passworte oder PIN-Codes zu merken. Damit aber werden diese **Zugangs- und Zugriffssicherungen** problematisch und ein Sicherheitsrisiko. Seit mehreren Jahren versucht deshalb die Industrie biometrische Verfahren wie die Gesichtserkennung für die Zugangskontrolle oder den Fingerabdruck für die Nutzung von PCs oder Handys zur Serienreife zu entwickeln. Einen besonderen Schub bekam diese Technik durch die Ereignisse des 11. Septembers 2001 mit der Erwartung, durch die Aufnahme derartiger Merkmale beispielsweise in Ausweisdokumente die Identifikation und Überprüfung (Verifikation) von Personen erheblich verbessern zu können.

Biometrische Merkmale sind individuelle Ausprägungen allgemeiner Körpermerkmale, die ein Leben lang unverändert erhalten bleiben. Sie können vermessen, aufgezeichnet, gespeichert und zum Zwecke der Identifizierung bestimmten Personen zugeordnet und mit den Merkmalen anderer Personen verglichen werden (siehe auch unter 12). Zu diesen Merkmalen gehören beispielsweise der Fingerabdruck, die Stimme, die Unterschrift, die Iris, das Gesicht, die Handgeometrie, der Körpergeruch. Sollen diese Merkmale aufgezeichnet und gespeichert werden, so werden sie nach der Erfassung auf die prägenden Elemente - so genannte „Templates" - reduziert. Beim Fingerabdruck sind dies beispielsweise die Minutien (prägende Punkte und Linien), beim Gesicht bestimmte geometrische Eckpunkte. Allen biometrischen Verfahren ist gemeinsam, dass sie **keine**

hundertprozentige Erkennung ermöglichen und auch bei einem bestimmten Prozentsatz der Menschen wegen unzureichender Ausprägung dieses Merkmals nicht anwendbar sind. Beispielsweise besitzen nach ersten wissenschaftlichen Erkenntnissen ca. 5 bis 10 % der Menschen nicht genügend Minutien, um eine Erkennung mittels eines Fingerabdruckverfahrens zu ermöglichen. Bei bundesweiten Ausweisdokumenten mit integriertem Fingerabdruck würde dies bedeuten, dass mindestens 2.500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Ersatzsystem für die Personen vorhanden sein, die eine sehr schlechte Merkmalausprägung besitzen oder überhaupt nicht erfasst werden können.

Zum Einsatz biometrischer Verfahren gibt es bisher keine statistisch validen Erkenntnisse. Aus der Praxis können lediglich Erfahrungen mit kleineren Systemen herangezogen werden (etwa die automatisierte Kontrolle durch die Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]). 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 für ein bestimmtes biometrisches Verfahren ist sehr aufwändig. Größere herstellerneutrale Untersuchungen gibt es bisher noch nicht. Dies betrifft auch Fragen der **Manipulationssicherheit** des Gesamtsystems. Insbesondere das Erkennen, ob das präsentierte Merkmal von einer lebenden Person stammt oder ob es sich hierbei um die Präsentation nachgebildeter Merkmale, wie beispielsweise die Silikonnachbildung eines Fingerabdrucks oder das Foto eines Gesichtes handelt, sind noch wenig ausgereift. Erst derartige Ergebnisse können belegen, ob einzelne biometrische Merkmale geeignet sind, die an sie gestellten Anforderungen zu erfüllen.

Werden biometrische Verfahren in das Ausweisdokument integriert, so ist zu befürchten, dass sich mit neu erfassten biometrischen Merkmalen oder mit den daraus generierten Datensätzen eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen lassen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise weder für weitere staatliche Zwecke (z. B. Strafverfolgung) noch 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 43).

Es ist deshalb insbesondere zu vermeiden, biometrische Daten in zentralen Referenzdateien zu hinterlegen. Oberstes Prinzip muss es sein, dass alle gespeicherten Merkmale in der alleinigen Verfügungsgewalt ihrer Besitzerinnen und Besitzer verbleiben. Besonders biometrische Rohdaten, also beispielsweise grafische Bilder von Fingerabdrücken, die nicht für die elektronische Identifikation genutzt werden, sollten nicht zusätzlich zentral gespeichert werden. Solche Datensammlungen unterliegen einem hohen **Missbrauchsrisiko** und sind deshalb abzulehnen. Biometrische Rohdaten lassen möglicherweise neben der Identifizierung auch völlig andere Auswertungen zu. So könnte aus Bildern des Gesichts, der Hand oder des Augenhintergrunds auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von verhaltensbasierten biometrischen Merkmalen wie der Sprache und der Unterschrift sowie in besonderer Weise von genetischen Daten. Für die Gewinnung der „Templates" erforderliche biometrische Rohdaten sind deshalb möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

Die Speicherung biometrischer Merkmale in zentralen Dateien könnte auch zu einer neuen Qualität der Überwachung führen. 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 der betroffenen Person handelt es sich hierbei um **nicht-kooperative Vorgänge**, die den betroffenen Personen 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 könnte. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nicht-kooperative, passive Systeme besonders abzulehnen.

Im Ergebnis zeigt sich, dass die Nutzung biometrischer Merkmale nicht unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal verwendet werden soll, müssen die verschiedenen Risiken sorgfältig gegeneinander abgewogen werden. Vor diesem Hintergrund

müssen gesetzliche Planungen, die die Nutzung biometrischer Merkmale zum Ziel haben, besonders streng auf ihre Verhältnismäßigkeit geprüft werden.

3.3 Sicherheitsanforderungen an Medizinnetze

Zur Steigerung von Qualität und Effizienz in der Gesundheitsversorgung sowie zur Kosteneinsparung spielt die einrichtungsübergreifende Kommunikation eine immer größere Rolle. Die folgenden Ausführungen sollen eine Hilfestellung zur Formulierung und Umsetzung einer Sicherheitspolitik für die elektronische Kommunikation im Gesundheitswesen bieten.

Anknüpfend an die Ausführungen im 14. und 15. Datenschutzbericht werden die verschiedenen Architekturen für Systeme zur einrichtungsübergreifenden Kommunikation aufgezeigt. Außerdem werden die essentiellen Sicherheitsmaßnahmen erläutert, die zur Erfüllung der Sicherheitsziele für Systeme zur medizinischen Datenverarbeitung erforderlich sind. Grundlegende Sicherheitsziele sind die Gewährleistung beziehungsweise Sicherstellung der Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit, Revisionsfähigkeit und Validität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten sowie der Rechtssicherheit im Hinblick auf die beweisbare Überprüfbarkeit von Verarbeitungsvorgängen, die Nicht-Abstreitbarkeit von Datenübermittlungen und die Nutzungsfestlegung im Sinne einer Festlegung von Nutzerkreisen mit abgestuften Nutzungsrechten und Nutzungsausschlüssen.

3.3.1 Formen der Datenhaltung

Im Folgenden werden Systemarchitekturen auf der Grundlage der Form ihrer Datenhaltung beschrieben. Es ist zu erwarten, dass jedes System zur einrichtungsübergreifenden Kommunikation einer dieser Kategorien zugeordnet werden kann oder sich als eine Kombination dieser Kategorien darstellt.

Bei der **dezentralen Datenhaltung** werden die Daten dort gespeichert, wo sie auch erzeugt wurden. Somit hat jede medizinische Einrichtung ihre eigene Datenhaltung. Die Datenhaltungssysteme der verschiedenen

Einrichtungen können zwar über ein Netz miteinander kommunizieren, sind aber ansonsten als vollständig autonom anzusehen. Systemübergreifende einheitliche Dienste gibt es nicht.

Bei der **zentralen Datenhaltung** werden Daten, deren Verarbeitung in der Verantwortung verschiedener medizinischer Einrichtungen liegt, (technisch) zentral zusammengeführt und nur in einem zentralen System gespeichert. Der Zugriffskontrollmechanismus gewährleistet, dass jede Einrichtung nur auf die eigenen Daten zugreifen kann. Will ein Mediziner der Einrichtung A ein Dokument X an eine Medizinerin der Einrichtung B übermitteln, veranlasst er, dass diese die Zugriffsrechte für dieses Dokument erhält.

Bei der **verteilten Datenhaltung** werden, wie im Falle der dezentralen Datenhaltung, die Daten auf den Systemen der Einrichtungen gespeichert, die sie auch erzeugt haben. Darüber hinaus gibt es aber systemübergreifende Dienste, die dafür sorgen, dass die einzelnen dezentralen Systeme zu einem Kommunikationsverbund zusammengeschlossen werden. Damit sind die dezentralen Systeme Subsysteme des Gesamtsystems. Den Nutzenden eines verteilten Systems bleibt die physikalische Verteilung der Daten auf eine Vielzahl von Subsystemen verborgen (Verteilungstransparenz) und ihnen wird der Eindruck vermittelt, als arbeiteten sie mit einem Zentralsystem. Ein verteiltes System benötigt Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente sowie einen systemweiten Zugriffskontrollmechanismus. Hierüber ist unabhängig vom Lagerort, bei entsprechender Berechtigung, der Zugriff auf alle Daten möglich.

Bei **dezentraler Datenhaltung mit zentraler Komponente** findet eine dezentrale Datenhaltung bei den einzelnen medizinischen Einrichtungen statt. Außerdem können Dokumente der verschiedenen Einrichtungen an einer zentralen Stelle temporär (technisch) zusammengeführt werden. Bei diesem Modell bildet die zentrale Speicherkomponente einen Puffer, der allen angeschlossenen Einrichtungen zum Up- und Download zur Verfügung steht. Dokumente werden von der Senderin oder vom Sender auf diesen zentralen Speicher übertragen (Upload) und können dann von der Empfängerin oder vom Empfänger von dort abgeholt (Download) werden.

3.3.2 Spezielle Datensicherheitsmaßnahmen

Grundsätzlich sind Sicherheitsmaßnahmen auf der Grundlage einer Bedrohungs- und Risikoanalyse individuell zu ermitteln. Unabhängig davon

sind die folgenden Maßnahmen aufgrund des hohen Schutzbedarfs medizinischer Daten als unabdingbar anzusehen.

Sicherstellung der Vertraulichkeit

Der Vertraulichkeit kommt aufgrund der hohen Sensibilität medizinischer Daten und der Pflicht zur Wahrung des Arzt-Patienten-Geheimnisses eine große Bedeutung zu. Insofern muss bei jeder Phase der Datenverarbeitung sichergestellt werden, dass nur befugte Personen patientenbezogene Daten zur Kenntnis nehmen können. Eine hinreichende Gewährleistung der Vertraulichkeit mit den hohen Anforderungen des Gesundheitswesens kann nur durch Verschlüsselung der patientenbezogenen Daten mit **starken kryptografischen Verfahren** erreicht werden. Zum einen ist eine Verschlüsselung aller Daten zu fordern, die über ein Kommunikationsnetz übertragen werden und zwar unabhängig davon, ob es sich um ein lokales oder um ein öffentliches Netz handelt. Daneben sind alle bei den datenhaltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass Systemadministration, Wartungspersonal oder sonstige Dritte (etwa durch Diebstahl) Kenntnis von Daten erhalten, die dem Arzt-Patienten-Geheimnis unterliegen.

(a) Verschlüsselung übertragener Daten

Die Übertragung patientenbezogener Daten in dezentralen Systemen erfordert eine **Verschlüsselung auf Anwendungsebene**. Da die Systeme in dezentralen Architekturen autonom sind und sich somit aus der Sicht eines Systems die übrigen Systeme jeweils wie Black Boxes darstellen, kann nur die an Personen adressierte Verschlüsselung sicherstellen, dass nur Befugte die übermittelten Daten zur Kenntnis nehmen können.

In zentralen Systemen reicht eine **Verschlüsselung auf Transportebene** aus, da alle Nutzerinnen und Nutzer dem Zugangs- und Zugriffskontrollmechanismus des Systems unterliegen.

In einem verteilten System reicht ebenso eine Verschlüsselung auf Transportebene aus, wenn es für den systemübergreifenden Datenaustausch einen einheitlichen, systemweiten Zugangs- und Zugriffskontrollmechanismus gibt.

Die dezentrale Architektur mit zentraler Komponente kann im Prinzip gehandhabt werden wie eine dezentrale Architektur, da die zentrale Komponente die Funktion eines „Postfaches" übernimmt, aus dem sich die Empfängerinnen und Empfänger ihre Nachrichten abholen.

(b) Verschlüsselung gespeicherter Daten

Die verschlüsselte Speicherung der Daten bei den datenhaltenden Systemen kann realisiert werden durch den Einsatz entsprechender Systemsoftware (beispielsweise Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (beispielsweise Tools zur Verschlüsselung von Plattenbereichen). Eine andere Möglichkeit zur Bewerkstelligung dieser Aufgabe besteht in der Verschlüsselung der patientenbezogenen Dokumente auf Anwendungsebene. Dabei bietet sich eine Hybridverschlüsselung an, wobei das Dokument selbst mit einem symmetrischen Schlüssel (Session Key) und der symmetrische Schlüssel jeweils mehrfach nach einem asymmetrischen Verfahren mit den öffentlichen Schlüsseln der **berechtigten Nutzerinnen und Nutzer** verschlüsselt wird. Die oder der für ein Dokument verantwortliche Medizinerin oder Mediziner legt dann (unter Umständen unter Mitwirkung der Patientin oder des Patienten) bei der Aktivierung des Verschlüsselungsvorgangs die berechtigten Personen fest. Diese Vorgehensweise stellt sicher, dass nur berechtigte Nutzerinnen und Nutzer in die Lage versetzt werden, ein Dokument zu entschlüsseln und realisiert damit gleichzeitig einen Zugriffskontrollmechanismus (bezogen auf Lesevorgänge). Das Verschlüsselungskonzept muss ein Verfahren vorsehen, das eine Verfügbarmachung der Daten im Notfall gewährleistet.

Gewährleistung der Authentizität

Patientenbezogene Dokumente sind von ihrer Urheberin oder ihrem Urheber beziehungsweise von der verantwortlichen Medizinerin oder dem verantwortlichen Mediziner elektronisch zu signieren und mit einem Zeitstempel zu versehen. Nur durch die **elektronische Signatur** kann die Zurechenbarkeit von Dokumenten zur Urheberin oder zum Urheber beziehungsweise zur Verantwortlichen oder zum Verantwortlichen sichergestellt werden. Die erforderlichen Mechanismen zur elektronischen Signatur von Dokumenten sind unabhängig von der gewählten Architektur der Datenhaltung.

Sicherstellung der Integrität

Mit dem elektronischen Signieren eines patientenbezogenen Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt, da der Signaturvorgang eine bewusste Handlung von der oder dem Signierenden erfordert. Das medizinische Personal, das ein Dokument elektronisch

signiert, also sozusagen elektronisch unterschreibt, bestätigt mit der Signatur nicht nur, dass sie oder er die Urheberin oder der Urheber beziehungsweise die oder der Verantwortliche ist, sondern gleichzeitig, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Darüber hinaus sichert das der elektronischen Signatur zugrunde liegende kryptografische Verfahren die Erkennbarkeit einer nachträglichen Veränderung eines Dokuments. Die erfolgreiche Verifikation der Signatur eines Dokuments stellt damit gleichzeitig die **Unversehrtheit** des Dokumenteninhalts sicher.

Sicherstellung der Verfügbarkeit

Bei der Sicherstellung der Verfügbarkeit teilen sich die verschiedenen Architekturansätze in zwei Lager:

Sowohl im Falle der zentralen Datenhaltung als auch im Falle der dezentralen Datenhaltung mit zentraler Komponente ist eine hohe Verfügbarkeit durch die zentrale Datenverarbeitungsanlage und damit für das **gesamte System** realisierbar. Bei dezentraler Datenhaltung mit zentraler Komponente können sich Einschränkungen der Verfügbarkeit des Gesamtsystems nur aus einer temporären Nichtverfügbarkeit von angeschlossenen dezentralen Systemen für einen notwendigen Upload oder Download ergeben.

Bei der dezentralen und verteilten Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit aller beteiligten **(Sub-)Systeme** ab. Insbesondere im niedergelassenen Bereich dürften sich die Verfügbarkeitszeiten der Systeme auf die Praxiszeiten beschränken, die zudem von Praxis zu Praxis noch unterschiedlich sein können. Bei der verteilten Datenhaltung müssen Kommunikationsprozesse – im Gegensatz zum dezentralen Fall – nicht explizit von den Nutzenden eines Subsystems initiiert werden, sondern können durch systemweit verfügbare Kommunikationsmechanismen angestoßen werden. Insofern wird die Verfügbarkeit nicht notwendigerweise von beschränkten Praxiszeiten determiniert. Allerdings kann es zu technisch bedingten Ausfällen von Subsystemen kommen, die ohne Eingriffe vor Ort nicht behebbar sind. Solchen Schwierigkeiten kann technisch dadurch begegnet werden, dass **Datenreplikate** an verschiedenen Speicherorten vorgehalten werden. Bei Nichtverfügbarkeit eines bestimmten Subsystems wird dann auf das entsprechende Replikat zurückgegriffen. Diese Vorgehensweise ist allerdings datenschutzrechtlich als sehr **problematisch** einzustufen, wenn die Replikate sich nicht im selben Herrschaftsbereich befinden wie ihre

Originale. Außerdem ergeben sich durch Replikate nicht zu unterschätzende Konsistenzprobleme.

Gewährleistung der Revisionsfähigkeit

Grundvoraussetzung für die Gewährleistung der Revisionsfähigkeit ist das **elektronische Signieren** der patientenbezogenen Dokumente, weil hiermit die Verantwortlichkeit beziehungsweise Urheberschaft anerkannt wird. Da der Inhalt eines signierten Dokuments nachträglich nicht mehr verändert werden kann, ohne die Signatur zu verletzen, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdokument plus Ergänzungen wiederum digital signiert, kann die Historie eines Dokuments manipulationssicher festgehalten werden.

Die von der Dokumentensignatur nicht erfassbaren Verarbeitungsschritte des Übermittelns eines Dokuments und des Lesens eines Dokuments sind mittels einer **manipulationssicheren Protokollierung** einer Revision zugänglich zu machen. Das vollständige Löschen eines Dokuments muss aus Gründen der Dokumentationspflicht in jedem Fall vom Zugriffskontrollmechanismus unterbunden werden.

Eine Protokollierung ist bei zentralen Systemen naturgemäß recht einfach und umfassend zu realisieren, da hierbei die Datenverarbeitung von nur einem System vorgenommen wird, welches damit auch die Kontrolle über alle Verarbeitungsphasen eines Dokuments hat und außerdem die einzelnen Verarbeitungsschritte den Personen zuordnen kann, die sie verursacht haben.

Hingegen durchläuft ein Dokument im Zuge seiner Verarbeitung bei einem **dezentralen System** unter Umständen mehrere lokale Systeme. Da es in einem dezentralen System keine zentrale Kontrollinstanz über die Verarbeitungsschritte der Einzelsysteme gibt, ist eine zentrale Protokollierung nicht möglich. Hier bleibt nur die **Protokollierung durch die lokalen Systeme**. Die Protokollierung von Lesevorgängen ist problemlos möglich. Die Protokollierung von Übermittlungsvorgängen erfordert allerdings Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangens von Dokumenten (dazu unten). Für die Revision der Gesamtheit aller Verarbeitungsschritte eines Dokuments ist allerdings das Zusammenführen der relevanten Protokolldaten aller lokaler Systeme erforderlich, die das Dokument durchlaufen hat.

Bei verteilten Systemen können systemweit zur Verfügung stehende Dienste zur Protokollierung von Verarbeitungsschritten genutzt werden, die systemübergreifende Wirkung haben (also im Wesentlichen Datenübermittlungen). Alle anderen Aktivitäten, die nicht von systemweiten Diensten abhängen, können wie in dezentralen Systemen nur von den beteiligten lokalen Subsystemen protokolliert werden.

Die dezentrale Datenhaltung mit zentraler Komponente erlaubt eine Protokollierung aller Aktivitäten, die sich auf die zentrale Komponente beziehen. Alle Aktivitäten, die sich auf die lokalen Systeme beschränken, müssen von diesen protokolliert werden. Die Protokollierung von Datenübermittlungen zwischen den lokalen Systemen und der zentralen Komponente erfordert wiederum Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten.

Gewährleistung der Validität

Die Sicherstellung der Validität ist prinzipiell unabhängig von der Architektur der beteiligten Systeme. Sie ist aber in hohem Maße abhängig von einer **Standardisierung** der für die Validität relevanten Systemkomponenten (Hard- und Softwarekomponenten). Insofern ist anzunehmen, dass eine valide Datenverarbeitung umso schwieriger herstellbar ist, je heterogener die zu betrachtende Systemlandschaft ist.

Gewährleistung der Rechtssicherheit

Die Voraussetzung für die Rechtssicherheit ist die Revisionsfähigkeit und damit auch das elektronische Signieren eines jeden patientenbezogenen Dokuments. Damit eine elektronische Signatur rechtsverbindlich einer verantwortlichen Person zugeordnet werden kann, bedarf es der **qualifizierten Signatur**. Erst die qualifizierte Signatur gewährleistet eine rechtswirksame Überprüfbarkeit der Zuordnung einer Signatur zu der Person, die diese Signatur erzeugt hat.

Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen

Die Nicht-Abstreitbarkeit des Sendens und Empfangens spielt primär eine Rolle in Architekturen mit dezentraler Ausrichtung, da aufgrund der Autonomie der lokalen Systeme eine Datenübermittlung explizit von einer Systemnutzerin oder einem Systemnutzer angestoßen werden muss und es keine systemübergreifenden Kontrollmechanismen gibt, die einen Übermittlungsvorgang technisch überwachen und im Fehlerfall entsprechende Maßnahmen einleiten. Nicht-Abstreitbarkeit ist nur über ein

Quittungsverfahren unter Verwendung elektronischer Signaturen zu realisieren. Die ein Dokument sendende Person versieht dieses zunächst mit einer elektronischen Signatur und sendet es an die empfangende Person. Die empfangende Person verifiziert die Signatur, um festzustellen, ob das Dokument von der angegebenen sendenden Person stammt. Dann muss die empfangende Person der sendenden Person bestätigen, dass sie ein Dokument mit bestimmtem Inhalt von ihr bekommen hat. Diese Empfangsbestätigung kann realisiert werden, indem von dem empfangenen Dokument der Hashwert gebildet wird und dieser zusammen mit einem das Dokument identifizierenden Merkmal (und eventuell mit der Eingangszeit) von der empfangenden Person elektronisch signiert an die sendende Person gesendet wird. Die sendende Person verifiziert die Signatur der Quittung, bildet ihrerseits den Hashwert des von ihr gesendeten Dokuments und vergleicht diesen mit dem in der Quittung zugesandten Hashwert. Stimmen beide Werte überein, kann die sendende Person sicher sein, dass genau die von ihr spezifizierte empfangende Person (aufgrund der Signaturverifikation) auch genau das von ihr gesendete Dokument (aufgrund des Vergleichs der Hashwerte) erhalten hat. Schlägt die Signaturverifikation oder der Hashwertvergleich fehl, muss sich die sendende Person mit der empfangenden Person in Verbindung setzen. Erhält die empfangende Person keine Reklamation durch die sendende Person, dann kann sie ihrerseits sicher sein, dass das empfangene Dokument genau von der vermuteten sendenden Person kommt, mit genau dem von der sendenden Person gesendeten Inhalt. Erhält bei diesem Quittungsverfahren die sendende Person nach einer gewissen Zeit keine Quittung für ihre gesendete Nachricht, so ist entweder die Nachricht oder die Quittung nicht zugestellt worden. Für diesen Fall ist eine adäquate Handlungsweise zu vereinbaren (beispielsweise erneutes Senden der Nachricht nach einer Wartefrist oder Kontaktieren der empfangenden Person).

Die Signatur von Dokumenten zur Sicherstellung der **Nicht-Abstreitbarkeit** von Datenübermittlungen darf nicht verwechselt werden mit der Signatur von Dokumenten zur Gewährleistung der **Authentizität**. Im ersten Fall dient die Signatur der Zuordnung eines Dokuments zur sendenden Person, im zweiten Fall der Zuordnung eines Dokuments zu seiner Urheberin oder seinem Urheber. Da die ein Dokument sendende Person aber nicht notwendigerweise auch die Urheberin oder der Urheber ist, muss jedes Dokument bei einer Übermittlung von der sendenden Person elektronisch signiert werden.

Gewährleistung der Nutzungsfestlegung

Da bei zentraler Datenhaltung der Zugriffskontrollmechanismus eine systemweite Kontrolle ausüben kann, ist eine Nutzungsfestlegung **prinzipiell umfassend** zu realisieren. Es kommt nur darauf an, welche Differenzierung das Berechtigungskonzept beziehungsweise die Zugriffskontrolle des jeweiligen Systems zulässt. Aufwändig könnte die Umsetzung eines Nutzungsausschlusses sein (beispielsweise leseberechtigt sind alle Medizinerinnen und Mediziner der Abteilung A mit Ausnahme von Dr. X der Abteilung A).

Existiert in einem System mit verteilter Datenhaltung ein systemweites Berechtigungskonzept und ein systemweiter Zugriffskontrollmechanismus, sind Nutzungsrechte, die systemübergreifende Bedeutung haben, wie bei einem Zentralsystem definierbar.

Bei dezentralen Systemen sind **Nutzungsrechte** mittels des Zugriffskontrollmechanismus jeweils für die lokalen Systeme definierbar. Wird ein Dokument von einem lokalen System an ein anderes übermittelt, müssen die unter Umständen bestehenden Nutzungsrechte beziehungsweise Nutzungsausschlüsse mit dem Dokument **übermittelt** werden. Die empfangende Person des Dokuments muss dann für deren Einhaltung sorgen.

Dezentrale Systeme mit zentraler Komponente können Zugriffskontrollmechanismen für die zentrale Komponente wie im zentralen Fall realisieren. Dokumente, die sich im Speicherbereich der Subsysteme befinden oder in deren Speicherbereich gelangen, entziehen sich dem zentralen Zugriffskontrollmechanismus und sind wie im dezentralen Fall zu behandeln.

3.4 Allzeit bereit - Risiken mobiler Kommunikation

Die mobile Kommunikation hat in unseren Alltag Einzug gehalten. Immer häufiger werden Dienste und Funktionen über mobile Endgeräte angeboten. Beim Telefonieren über Handy oder schnurloses Telefon, bei der Nutzung von Navigationssystemen, beim Abruf und Versenden von Informationen und persönlichen Nachrichten von beliebigen Orten über Laptops bis hin zum aus der Ferne gesteuerten vollautomatischen Haushalt, der selbstständig darüber wacht, welche Bestellungen per Internet erfolgen müssen - überall ist der Funk die Basis der Übertragung. Da in vielen Bereichen personenbezogene Daten

und Informationen übertragen werden, ist der Schutz dieser Daten von großer Bedeutung.

Aufgrund der systembedingten Schwäche der Funkübertragung - der offenen und damit für viele zugänglichen Ausstrahlung - sind in erster Linie im Netz ausreichende Sicherheitstechniken zur Wahrung der Vertraulichkeit, Integrität und Authentizität der Daten und der bewusste Umgang mit den Schutzmechanismen erforderlich. Daneben sind die Gerätefunktionen und die Kommunikation so aufzubauen, dass den Nutzenden immer bewusst ist, welche Daten sie gegenüber den Diensteanbietenden preisgeben.

Technische Grundlage der mobilen Kommunikationstechnologien sind die öffentlichen Zellnetze GSM oder UMTS sowie die lokalen Netze Wireless LAN (WLAN) oder Bluetooth. Je nach eingesetzter Technik und Anwendungsfeld sind die grundlegenden Sicherheitsmechanismen, Regeln und Funktionen unterschiedlich.

UMTS

UMTS (Universal Mobile Telecommunications System) wird auch als die dritte Generation des Mobilfunks (3G) bezeichnet. UMTS basiert auf dem so genannten WCDMA-Verfahren (Wideband Code Division Multiple Access) bei dem alle Daten innerhalb einer Funkzelle auf derselben Frequenz übertragen werden. Die entscheidende Verbesserung bei der UMTS-Technologie liegt in der **Bandbreite** der genutzten Frequenzen. Sie liegt bei 5 MHz - das ist der 25fache Wert gegenüber dem bisherigen Sprachfunknetz. Damit sind Übertragungsraten bis zu 2 MBit/s möglich.

Zudem zeichnen sich UMTS-Netze durch eine **neuartige Zellenstruktur** aus. Die kleinste Zelle ist die Picozelle mit einem Durchmesser von unter hundert Metern. Mit Picozellen werden beispielsweise so genannte 'hot spots', Bürogebäude, Hotels, Flughäfen oder Messen versorgt. Die Mikrozelle mit einer Ausdehnung von bis zu mehreren Kilometern versorgt ganze Stadtbereiche. Für Vororte gibt es die Makrozelle mit einer Reichweite von über 20 Kilometern. Hyper- und Umbrella-Zellen, die im globalen Konzept von UMTS auch als Weltzellen bezeichnet werden, können eine Ausdehnung von bis zu mehreren hundert Kilometern haben.

Die neue, feinere Zellaufteilung und die höhere Bandbreite sind Basis für die neuen Dienste. Videos per Handy, Internet im Hyper-Speed, umfangreiche Informationen in Sekunden abrufbar, mobiles Banking mit Aktiencharts und biometrischer Verifizierung. Fachleute erwarten eine

stärkere Verbreitung der ortsbezogenen Dienste - Location Based Services (LBS) - die sich auf die besseren Ortungsfunktionen des UMTS-Netzes stützen. Möglich wäre beispielsweise die Übertragung von Kartenausschnitten etwa zur nächsten U-Bahn-Haltestelle oder die Information über eine naheliegende Apotheke. Gerade diese neuen **Ortsbestimmungsfunktionen** beinhalten umgekehrt aber auch die verstärkte Möglichkeit der **Überwachung** und Kontrolle. Sie sind besonders kritisch zu betrachten.

Wireless-LAN

Wireless-LAN (WLAN) oder auch Funk-LAN genannt kann in verschiedenen Architekturen betrieben werden. Die einfachste Art ist der **Ad-hoc-Modus**. Hierbei kommunizieren zwei oder mehrere Clients direkt miteinander. Eine LAN-Infrastruktur ist hierfür nicht erforderlich. In den meisten Fällen wird ein WLAN im **Infrastruktur-Modus** betrieben. Das heißt, die Kommunikation der Clients erfolgt über eine zentrale Funkbrücke, dem so genannten Access-Point. Dieser dient als Repeater, verdoppelt die Funkreichweite und stellt die Verbindung zum kabelgebundenen LAN her. Die Reichweite einer Funkzelle beträgt - abhängig von den Umgebungsbedingungen - circa 30 - 150 Meter.

WLAN-Systeme beinhalten bezüglich der Sicherheit große Risiken. Viele Sicherheitsmechanismen sind schwach und zusätzlich im Auslieferungszustand nicht aktiviert. So kann beispielsweise die MAC-Adresse der Funk-Clients relativ einfach abgehört und für Manipulationen genutzt werden. Zum Zwecke des Zugriffsschutzes häufig eingebaute MAC-Adressfilter sind somit leicht überwindbar.

Um die Vertraulichkeit der zu übertragenden Daten zu wahren, können diese optional über das Verfahren Wired Equivalent Privacy (WEP) verschlüsselt werden. Bei Nutzung der Verschlüsselung ist jedoch darauf zu achten, dass mit einer **ausreichenden Schlüssellänge** gearbeitet wird. Erst neuere Geräte nutzen eine Schlüssellänge von 128 bit. Wird diese Option nicht aktiviert, erfolgt eine unverschlüsselte Übertragung. Dies ermöglicht es Dritten, die Kommunikation abzuhören, indem sie beispielsweise eine Wireless LAN Karte in ihrem PC installieren und sich damit Zugriff auf ein WLAN verschaffen.

Eine weitere Schwachstelle im WEP-Protokoll ist das nicht automatisierte Schlüsselmanagement. Schlüssel müssen in einem Netz „von Hand" verteilt werden. In jedem Client (beispielsweise auf der Anschlusskarte oder auf der

Festplatte) und im Access-Point muss der gleiche statische Schlüssel eingetragen werden. Da hiermit ein physischer Zugriff auf die Komponenten verbunden ist, bedeutet dies, dass in der Praxis der geheime Schlüssel nur selten oder überhaupt nicht gewechselt wird. Die Offenbarung eines Schlüssels, beispielsweise durch Verlust eines Clients oder mittels frei verfügbarer Tools, kompromittiert sämtliche Schlüssel des gesamten WLAN.

Bei den am WLAN angeschlossenen Clients entstehen zusätzliche **Bedrohungen für die lokalen Daten**. Lokale Datei- oder Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung, meist auch über das WLAN, Zugriffe auf diese Ressourcen. Ebenso ist Hacking zu befürchten, bei dem Schwachstellen des verwendeten Betriebssystems ausgenutzt werden.

Daneben können WLANs wegen der Funkübertragung **leicht gestört** werden. Sie besitzen deshalb die den Funknetzen eigene, nur geringere Verfügbarkeit.

Bluetooth

Die Bluetooth Technik ist für drahtlose Verbindungen im Nahbereich (Pico-Netz) bis zu einer Reichweite von 10 Metern einsetzbar. Mit dieser Technik lassen sich besonders Peripherie-Geräte bequem kabellos koppeln. In vielen neuen Produkten wie in Notebook-Erweiterungen, PC-Karten, Handys, Druckern, Kameras oder PDAs (Personal Digital Assistant) gibt es inzwischen bereits Bluetooth Module. Damit Bluetooth so verschiedene Aufgaben wie Druckeransteuerung, Sprachübertragung oder die E-Mail-Kommunikation erledigen kann, müssen Bluetooth-Geräte eine **umfangreiche Spezifikation** erfüllen. Diese besteht aus vielen aufeinander gestapelten Protokollen, die von der Anwendungsschnittstelle bis hinab zum Funkteil (Radio) reichen. Bluetooth funkt im lizenzfreien 2,4-GHz-Band (ISM, Industrial/Scientifical/Medical) und wechselt 1600 Mal pro Sekunde nach einem komplexen Muster die Frequenz (Frequency Hopping Spread Spectrum, FHSS). Dies soll eine gewisse Robustheit gegenüber Störungen bieten und auch das Abhören erschweren.

Bluetooth garantiert die Sicherheit auf der Bitübertragungsebene. Authentifizierungs- und Verschlüsselungsmechanismen sind in jedem Bluetooth Gerät identisch implementiert. Die Authentifizierung mit einem 128-Bit-Schlüssel zwischen Bluetooth Devices erfolgt optional durch die Nutzenden. Sie kann uni- oder bidirektional eingerichtet werden. Diese

Informationen lassen sich speichern und automatisieren. So ist es möglich, das eigene Handy vom eigenen Notebook ohne Beschränkung nutzen zu lassen, eine weitere Nutzung jedoch zu untersagen. Die Verschlüsselung erfolgt zur Sicherung des Funkverkehrs. Je nach Einstellung beinhaltet sie Schlüssellängen von 8 bis 128 Bit. Ist eine höhere Sicherheit nötig, können zusätzliche Sicherheitsmechanismen der auf Bluetooth aufsetzenden Netzwerkprotokolle oder zusätzliche Verschlüsselungssoftware verwendet werden.

Allgegenwärtige Datenverarbeitung

Mobile Geräte, heute schon bekannt als Handhelds, PDAs oder Organizer, sowie kleine Computer in verschiedensten Geräten - so genannte Embedded Systems - werden in Zukunft unser Leben beeinflussen. Da solche Geräte uns überall - beispielsweise im Haushalt, im Auto, auf Reisen - begegnen werden, spricht man auch von Ubiquitous (allgegenwärtig), Pervasive (durchgehend) oder Ambient (umgebend) Computing.

Basistechnologie für diese Art der Datenverarbeitung sind neue, sehr kleine mobile Endgeräte, die beispielsweise in beliebige Alltagsgegenstände integriert sind und die mit Hilfe von Sensoren ihr Umfeld erfassen. Mobile Kommunikationstechnologien ermöglichen die **Vernetzung** dieser Endgeräte und somit den **grenzenlosen Datenaustausch** zwischen ihnen. Die Anwendungen selbst werden in den verschiedenen Systemebenen verteilt ausgeführt, so dass es an mehreren Stellen zu Verarbeitungen und Datenhaltungen kommt. Derartige Nutzungsformen hinterlassen viele **Datenspuren** und bergen somit viele **Risiken**.

Bereits in den heutigen mobilen Kommunikationsgeräten werden persönliche Daten unterschiedlichster Qualität verarbeitet. So sind in vielen Handys und PDAs Adresslisten, elektronische Merkzettel, Einkaufslisten, persönliche Informationen, Navigationen und auch Informationen für Bezahlverfahren gespeichert. Die Weitergabe und Verarbeitung dieser Daten könnte somit Aufschluss über Aktivitäten, Aufenthaltsorte und -zeiten, Bewegungen, Kommunikationspartnerinnen und -partner sowie das soziale Umfeld der Nutzenden geben.

Eine höhere Transparenz und Sicherheit kann bei der Nutzung von Netzdiensten erreicht werden, wenn in Anlehnung an den **Internet-Standard P3P** (Platform of Privacy Preferences) zu Beginn über Art, Umfang und Nutzung der erforderlichen Daten informiert wird und eine individuelle, dienstspezifische Einwilligung oder Ablehnung für die

Weitergabe von Informationen erfolgt. Daten werden nur dann übermittelt, wenn die Anforderungen von Nutzenden und Anbietenden im Einklang stehen. Durch diese Art der Kommunikation haben die Nutzenden **selbst die Wahl**, den Grad der Unbeobachtbarkeit, Vertraulichkeit, Anonymität oder Pseudonymität festzulegen. Implementiert werden kann ein solches persönliches Profilmanagement funktional sowohl in den Endgeräten als auch in den Diensteangeboten.

3.5 Einzelfragen zur Datensicherheit

3.5.1 Outsourcing von Verwaltungsnetzen

Immer häufiger werden in Verwaltungen IT-Infrastrukturen darauf überprüft, ob sie kostengünstiger betrieben werden können. Hierbei spielt der Aspekt des Outsourcing eine große Rolle. Überlegungen in diese Richtung betreffen den Datenschutz insbesondere deshalb, weil es durch die Aufgabenverlagerung auf Dritte auch zu einer Übermittlung der Daten kommt und damit die Möglichkeit der unbefugten Einsichtnahme, Nutzung und des Missbrauchs erleichtert wird.

Innerhalb der Landesregierung bestanden im Berichtszeitraum Überlegungen zum Outsourcing des Landesverwaltungsnetzes (LVN) in der Form, dass die Bereitstellung und der Betrieb des IP-Netzes durch private Telekommunikationsanbieter erfolgen sollte. Da über das Landesverwaltungsnetz auch verschiedene Verfahren mit personenbezogenen Daten betrieben werden, die einem besonderen Amtsgeheimnis unterliegen (Steuerdaten, Sozialdaten), ist der **Schutz der Vertraulichkeit** dieser Daten von besonderer Bedeutung. Werden die Daten nicht verschlüsselt, kann bei einem Übergang der Systemverantwortung für das Datennetz auf private TK-Anbieter selbst bei Einhaltung hoher Sicherheitsauflagen nicht verhindert werden, dass die Telekommunikationsanbieter die über das Netz übertragenen Daten zur Kenntnis nehmen können. Zwar besteht das Datenschutzrisiko der unbefugten Einsichtnahme Dritter in Daten bereits dann, wenn lediglich die für die Datenfernverarbeitung genutzten Datenleitungen von TK-Anbietern angemietet werden. Es erhöht sich jedoch erheblich bei Bereitstellung und Betrieb des Netzes durch Dritte.

Das Innenministerium als federführendes Ressort wurde darauf hingewiesen, dass bei einem derartigen Outsourcing-Vorhaben allein durch

vertragliche Maßnahmen der Datenschutz nicht hinreichend sichergestellt wird. Das DSG NRW sieht in § 10 vor, dass auch die geeigneten technischen Maßnahmen zu treffen sind, um den Schutz der Daten zu gewährleisten. Das wäre in diesem Fall der Einsatz von **Verschlüsselungs-** und **Signaturverfahren**, die außerhalb des Verantwortungsbereichs des Netzbetreibers liegen. Sie stellen sicher, dass insbesondere die Vertraulichkeit der Daten gewährleistet wird und eine unbefugte Kenntnisnahme nicht erfolgen kann. Geeignete Produkte auf der Transport- oder Anwendungsebene sind am Markt erhältlich. Hieraus ergibt sich die **Verpflichtung**, sie zur Minderung der Datenschutzrisiken zeitnah einzusetzen. Es ist allerdings notwendig, diese Produkte in die bestehenden Verfahren einzubinden.

In dem oben beschriebenen Fall kam es nicht zum Outsourcing des LVN. Unabhängig davon ist darauf hinzuweisen, dass durch die Privatisierung im Telekommunikationsbereich und die Einbeziehung Dritter in fast alle Datenfernverarbeitungsvorgänge durch die Anmietung oder Nutzung von Leitungen es notwendig und auch machbar ist, zu übertragende Daten besser zu schützen.

Es kann auf Dauer nicht akzeptiert werden, dass unter Zugrundelegung alter Sicherheitsüberlegungen aus den siebziger Jahren Daten offen, also ungeschützt, über Netze übertragen werden. Insbesondere bei neuen Verfahren sollte von Beginn an die Einbindung von Verschlüsselungsverfahren verfolgt werden. Eine technische Realisierung ist möglich und die erforderlichen Produkte sind vorhanden.

3.5.2 Anwendungsfehler: Kleine Ursache - großer Schaden für den Datenschutz

In einigen Beschwerdefällen führten offensichtlich Bedienungsfehler in den verwendeten Programmen zu einer Versendung von vertraulichen Unterlagen an unbeteiligte Dritte. Ursache war eine fehlerhafte Zuordnung von Datensätzen zu Adresslisten aufgrund gleichlautender Nachnamen. Zur Begrenzung derartiger Schäden sollten in den eingesetzten Programmen Funktionalitäten oder geeignete Plausibilitätsprüfungen integriert werden, die helfen, **Bedienungsfehlern** vorbeugend **entgegenzuwirken**. Beispielsweise ist es hinsichtlich der gesetzlich geforderten Revisionsfähigkeit nicht akzeptabel, wenn bei der Namenseingabe für eine Registerauskunft programmbedingt zunächst nur ein Datensatz als Treffer zur Weiterverarbei-

tung angeboten wird, obwohl mehrere Datensätze zum eingegebenen Namen existieren. Dies kann bei oberflächlicher Bearbeitung schnell zu falschen Zuordnungen führen.

In einem anderen Fall wurden durch **fehlerhafte Anwendungsprogrammierung** Adress- mit Namensdateien falsch verknüpft, so dass sensible personenbezogene Daten an unbeteiligte Dritte gesendet wurden. Hier zeigt sich erneut, dass **Test und Freigabe** auch bei einfachen Programmen oder individuellen Arbeitshilfen zwingend notwendig sind.

3.5.3 Datensicherheit auf FTP-Servern

Obwohl das Thema Datensicherheit im Internet seit geraumer Zeit große Aufmerksamkeit in der Presse erfährt, verwundert es doch sehr, wenn sensible personenbezogene Daten ohne **besondere Schutzmaßnahmen** auf einem offenen FTP-Server zwecks Datenübermittlung abgelegt und dort schlichtweg vergessen werden. Da FTP-Server mit offenem Zugang in der Regel genutzt werden, um Internetnutzerinnen und -nutzern Informationen, Daten und Programme allgemein zur Verfügung zu stellen, bestand für alle die Möglichkeit des Zugriffs auf diese Daten. Darüber hinaus ist bekannt, dass FTP-Server zu den bevorzugten **Angriffszielen** von Hackern zählen.

Das Beispiel zeigt, dass nach wie vor trotz aller getroffenen technischen und organisatorischen Maßnahmen die Schwachstelle Mensch bleibt. Sicherheitskonzepte, wie sie auch in § 10 Abs. 3 DSG NRW gefordert werden, sollten dies in stärkerem Maß berücksichtigen. Die erfolgreiche Erarbeitung und Realisierung eines Sicherheitskonzepts setzt allerdings voraus, dass Behörden- und Geschäftsleitungen die **Datensicherheit als Unternehmensziel** in ihrer Geschäftspolitik fest verankern. Unternehmen und auch öffentliche Stellen können es sich auf Dauer nicht leisten, Aspekte der Datensicherheit insbesondere bei der Auftragsdatenverarbeitung unberücksichtigt zu lassen.

3.5.4 Alle Jahre wieder

Datenschutzverstöße beispielsweise beim Versenden und Empfangen von **Telefaxen** und **Briefpost** sowie bei der **Unterlagenvernichtung** sind ein **Dauerthema** und könnten als ständige Rubriken einen festen Platz in den

Datenschutzberichten einnehmen. Manche mögen das Thema als monotone Wiederholung abtun, Resignation ist allerdings hier völlig fehl am Platz. Die Vielzahl der berechtigten Beschwerden besorgter Bürgerinnen und Bürger bestätigt die Notwendigkeit, weiterhin auf diese Missstände aufmerksam zu machen und Aufklärungsarbeit zu leisten.

Der fahrlässige Umgang mit personenbezogenen Daten bei deren **Übertragung mittels Telefax** war in der Vergangenheit wieder Gegenstand häufiger Beschwerden. So landeten beispielsweise Telefaxe mit personenbezogenen Daten aus dem Sozial- und Bankenbereich wie auch als vertraulich gekennzeichnete Dokumente bei unbeteiligten Dritten. Häufigste Ursache waren Anwahlfehler wegen fehlender Prüfung. Daneben wurde auch häufig von den öffentlichen und nicht-öffentlichen Stellen die Auffassung vertreten, dass für die Gewährleistung der Datensicherheit an der Empfangsstelle nicht die Absendenden, sondern allein die Empfängerinnen und Empfänger verantwortlich seien. Auch sei bei einer Telefaxbeantwortung davon auszugehen, dass die auf dem Fax angegebene Telefaxnummer den Betroffenen oder den von ihnen Beauftragten sicher zuzurechnen ist. Beide Auffassungen sind aus der Sicht des Datenschutzes nicht vertretbar. Eine Übertragung von Unterlagen mit sensiblen personenbezogenen Daten sollte nur in **Ausnahmesituationen** und nur dann durchgeführt werden, wenn die absendende Person nicht nur weiß, dass die Verbindung zur richtigen Empfangsstelle hergestellt wurde, sondern wenn ihr auch bekannt ist, dass das Telefax direkt von der berechtigten Person entgegengenommen wird. Informationen über die zu treffenden Sicherheitsvorkehrungen können der Orientierungshilfe „Datensicherheit beim Telefaxverkehr" im Internet unter www.lfd.nrw.de entnommen werden.

Bei der **Briefversendung personenbezogener Unterlagen** reicht das Spektrum der Beschwerden vom unsachgemäßen Verschließen der Briefumschläge, der offenen Versendung per Postkarte, der Versendung an unbeteiligte Dritte wegen Kuvertierungsfehlern bis hin zu zusätzlichen sachbezogenen oder auch diskriminierenden Angaben auf den Briefumschlägen oder in den Sichtfenstern. Zusätzliche Angaben neben der Anschrift auf Briefumschlägen oder in deren Sichtfenstern sind in der Regel für die Versendung nicht erforderlich und verletzen die schutzwürdigen Interessen der Empfängerinnen und Empfänger. Beim Versand ist deshalb dafür Sorge zu tragen, dass bei der Gestaltung des Adressen-Layouts keine datenschutzrechtlichen Bestimmungen verletzt werden. Arbeitsfehler beim

Postversand können erfahrungsgemäß angesichts des Massengeschäfts auch in Zukunft nicht ausgeschlossen werden. Allerdings kann durch die Einhaltung präventiver Maßnahmen die Wahrscheinlichkeit für das Auftreten derartiger Fehler stark verringert werden. Zu empfehlende Maßnahmen sind beispielsweise **Stichprobenkontrollen** nach der Kuvertierung und Prüfung der Funktionsfähigkeit der Gummierung der Umschläge einschließlich der Prüfung der Lagerbedingungen von Briefumschlägen, da schlechte Lagerbedingungen (Temperatur, Luftfeuchtigkeit) die Klebewirkung nachteilig beeinflussen können.

Bei der Vernichtung von **Unterlagen mit personenbezogenen Daten** ist häufig eine **große Sorglosigkeit** zu beobachten. Entsorgung von Aktenordnern mit sensiblen personenbezogenen Daten auf einer wilden Müllkippe oder über offene Papiercontainer sind keine Seltenheit. Mit der Realisierung von einfachen Maßnahmen - wie beispielsweise der Anschaffung von geeigneten Aktenvernichtern und der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für das Thema Datensicherheit - kann die Gewährleistung der Datensicherheit schon erheblich verbessert werden. Falls die Vernichtung größerer Aktenbestände nicht in Eigenregie durchgeführt werden kann, ist die Beauftragung von geeigneten Aktenvernichtungsunternehmen möglich (15. Datenschutzbericht 2001 unter 2.6.3, S. 55 ff. und die Orientierungshilfe zur Unterlagenvernichtung unter www.lfd.nrw.de).

4 Neues Bundesdatenschutzgesetz

Die Novelle des BDSG, mit der die EG-Datenschutzrichtlinie für Bundesbehörden und die Privatwirtschaft in nationales Recht umgesetzt wurde, ist am 23. Mai 2001 in Kraft getreten.

Im Folgenden soll ein kurzer Überblick über die wesentlichen Änderungen gegeben werden, soweit sie sich auf die Regelungen für nicht-öffentliche Stellen beziehen: Der Anwendungsbereich des BDSG umfasst nunmehr **alle Datenverarbeitungsvorgänge** unter Einsatz von Datenverarbeitungsanlagen oder aus nicht automatisierten Dateien, es sei denn, sie erfolgen ausschließlich für persönliche oder familiäre Tätigkeiten. Klargestellt ist in mehreren Vorschriften (beispielsweise in §§ 4 Abs. 1, 28 Abs. 1, 29 Abs. 1 BDSG), dass bereits das **Erheben** personenbezogener Daten den Regeln und Zulässigkeitsvoraussetzungen des BDSG unterliegt. Neu eingeführt wird in § 3 Abs. 9 BDSG der Begriff der **„besonderen Arten personenbezogener Daten"**, zu denen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben gehören. Diese Daten unterliegen besonders strengen Erhebungs- und Verarbeitungsregeln.

§ 3a BDSG formuliert den Grundsatz der **Datenvermeidung und Datensparsamkeit**. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel zu orientieren, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist, soweit es mit einem vertretbaren Aufwand zu realisieren ist, von den Möglichkeiten der Anonymisierung oder Pseudonymisierung Gebrauch zu machen.

An dem schon bestehenden **Verbot mit Erlaubnisvorbehalt**, nämlich dass die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat, hat sich nur insoweit etwas geändert, als auch die **Erhebung** der Daten denselben Voraussetzungen unterworfen ist (§ 4 Abs. 1 BDSG). In Abs. 2 der Vorschrift ist der aus dem öffentlichen Bereich stammende Grundsatz, wonach personenbezogene Daten bei der betroffenen Person zu erheben sind, auf die nicht-öffentlichen Stellen ausgedehnt worden. Ausnahmen von der **Direkterhebung bei den Betroffenen** sind auf wenige Fallkonstellationen beschränkt. Neu sind ebenfalls die in Abs. 3 geregelten Unterrichtungspflichten im Falle der Direkterhebung. Soweit die betroffene Person nicht bereits auf andere Weise

Kenntnis erhalten hat, ist sie über die Identität der verantwortlichen Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung und die Kategorien von Empfängerinnen und Empfängern zu unterrichten. Die Information über die Empfängerkategorien kann ausnahmsweise unterbleiben, wenn die Betroffenen mit einer Übermittlung an diese rechnen müssen.

Neu eingeführt wurde eine Vorschrift zur **Videoüberwachung** (§ 6b BDSG, siehe hierzu unter 5). Danach ist die Beobachtung öffentlich zugänglicher Räume zur Wahrnehmung des Hausrechts oder berechtigter Interessen zulässig. Die Zwecke müssen konkret festgelegt sein. Unzulässig ist die Beobachtung, wenn schutzwürdige Interessen der Betroffenen überwiegen. Die verantwortliche Stelle muss auf die Tatsache der Beobachtung hinweisen. Die Verarbeitung oder Nutzung der so erhobenen Daten, wie beispielsweise eine Video*aufzeichnung* und die Weitergabe an Strafverfolgungsbehörden, unterliegen weiteren Zulässigkeitsvoraussetzungen.

Sowohl bei der Datenverarbeitung und -nutzung für eigene Zwecke als auch zum Zwecke der Übermittlung (§§ 28, 29 BDSG) ist die **Zweckbindung** nunmehr strenger festgeschrieben, indem die jeweils verantwortliche Stelle verpflichtet wird, bereits bei der Datenerhebung konkret festzulegen, für welche Zwecke die Verarbeitung erfolgen soll. Zweckändernde Übermittlungen oder Nutzungen sind nur unter besonderen Voraussetzungen möglich.

Das bereits bestehende **Widerspruchsrecht** der Betroffenen gegen die Nutzung oder Übermittlung ihrer Daten zu Werbezwecken ist um eine Unterrichtungspflicht über dieses Recht ergänzt worden (§ 28 Abs. 4 Satz 2 BDSG, siehe hierzu unter 8.3.1). Die **Unterrichtung** muss bei der Ansprache zum Zwecke der Werbung erfolgen und umfasst die Nennung der verantwortlichen Stelle, bei der der Widerspruch eingelegt werden kann. Eine Verletzung der Unterrichtungspflicht ist gemäß § 43 Abs. 1 Nr. 3 BDSG eine Ordnungswidrigkeit und kann mit einer Geldbuße bis zu 25.000 € geahndet werden.

Mit der Änderung des BDSG sind auch die Befugnisse der Aufsichtsbehörden erweitert worden. War bisher lediglich eine Kontrolle möglich, wenn hinreichende Anhaltspunkte für die Verletzung von Datenschutzvorschriften vorlagen, ist die Aufsichtsbehörde nunmehr befugt, **Kontrollen ohne konkreten Anlass** durchzuführen. Die Ordnungswidrigkeitentatbestände sind gegenüber dem früheren Recht

erheblich ausgedehnt und die Höhe der Geldbußen in Teilbereichen deutlich angehoben worden. Neu ist auch, dass neben der oder dem Betroffenen auch die Aufsichtsbehörde für die in § 44 Abs. 1 BDSG geregelten Straftatbestände das Recht hat, Strafantrag zu stellen.

Es gibt schließlich umfangreiche Änderungen im BDSG, die den **internationalen Datenverkehr** betreffen. Beispielsweise besteht nunmehr gemäß § 4c Abs. 2 BDSG eine Genehmigungspflicht für bestimmte Datenübermittlungen in das Ausland. Da bisher nur vereinzelt Unternehmen einen solchen Antrag gestellt haben, ist davon auszugehen, dass die neuen Regelungen für den internationalen Datenverkehr noch nicht überall bekannt sind. Daher werden sie hier etwas ausführlicher dargestellt:

Erstmalig ausdrücklich geregelt wird in § 1 Abs. 5 BDSG die Frage, ob das BDSG anwendbar ist, wenn Daten in Deutschland **von einer ausländischen Stelle** erhoben werden. Unabhängig davon in welchem Land die für die Datenverarbeitung verantwortliche Stelle ihren Sitz hat, findet danach das BDSG immer Anwendung, wenn die Datenverarbeitung durch eine Niederlassung **in Deutschland** vorgenommen wird, auch wenn diese Niederlassung rechtlich unselbstständig ist. Werden Daten hingegen unmittelbar aus dem Ausland, beispielsweise via Internet oder Telefon, in Deutschland erhoben oder in sonstiger Weise verarbeitet, ist zu unterscheiden, ob die für die Datenverarbeitung verantwortliche Stelle ihren **Sitz in einem EU/EWR-Staat** hat oder ob es sich um eine Stelle in einem so genannten Drittstaat handelt. Am Abkommen über den Europäischen Wirtschaftsraum - EWR - sind derzeit außer den EU-Mitgliedstaaten auch Norwegen, Liechtenstein und Island beteiligt. Das BDSG geht im Anschluss an die EG-Datenschutzrichtlinie (Richtlinie 95/46/EG) davon aus, dass alle Staaten in der Europäischen Union und im übrigen Europäischen Wirtschaftsraum ein angemessenes Datenschutzniveau besitzen und die Persönlichkeitsrechte ausreichend schützen. Daher kann ohne Nachteile für den Schutz der Rechte der Einzelnen jeweils das Datenschutzrecht des Landes Anwendung finden, von dem aus eine verantwortliche Stelle Daten erhebt, auch wenn die Datenerhebung selbst in Deutschland geschieht. Hat eine datenerhebende Stelle hingegen ihren **Sitz in einem Drittland**, findet das BDSG immer auf Datenerhebungen und -verarbeitungen in Deutschland Anwendung, auch wenn die Stelle ausschließlich von ihrem Heimatstaat aus agiert. Diese Regelung verhindert, dass sich Firmen dem Anwendungsbereich des BDSG entziehen, indem sie zum Beispiel Server

im Ausland betreiben und von dort Daten über Personen in Deutschland via Internet erheben und verarbeiten.

Bei einer **Übermittlung von personenbezogenen Daten** von einer deutschen **an eine ausländische Stelle** ist ebenfalls die Unterscheidung zwischen EU/EWR-Staaten und Drittstaaten (beispielsweise USA) relevant. Stellen in einem Staat des Europäischen Wirtschaftsraums sind wie verantwortliche Stellen im Inland zu behandeln (§ 4b Abs. 1 BDSG).

Sollen personenbezogene Daten hingegen an eine Stelle übermittelt werden, die in einem Drittstaat liegt, muss nicht nur die Übermittlung selbst materiell nach datenschutzrechtlichen Vorschriften zulässig sein. Es muss grundsätzlich gewährleistet sein, dass bei der Stelle im Drittstaat, an die übermittelt werden soll, ein angemessenes Datenschutzniveau besteht (§ 4b Abs. 2 Satz 2 BDSG). Die **Angemessenheit des Datenschutzniveaus** im Drittstaat ist von der Stelle zu beurteilen, die die Daten übermitteln will (§ 4b Abs. 5 BDSG). Kriterien für die Beurteilung des Datenschutzniveaus enthält § 4b Abs. 3 BDSG. Ergänzend kann das Arbeitspapier WP 12 der Gruppe nach Art. 29 EG-Datenschutzrichtlinie herangezogen werden (abrufbar unter www.europa.eu.int).

Bereits durch Entscheidungen der EU-Kommission gemäß Art. 25 Abs. 6 EG-Datenschutzrichtlinie ist festgestellt und bedarf insofern keiner weiteren Überprüfung durch die datenübermittelnde Stelle, dass die Schweiz und Ungarn ein angemessenes Datenschutzniveau besitzen (Entscheidungen 2000/518/EG und 2000/519 EG vom 26. Juli 2000). Für Kanada hat die Kommission ebenfalls eine Entscheidung getroffen, wonach bei den Stellen, die dem "Canadian Personal Information Protection and Electronic Documents Act" unterliegen, ein angemessenes Schutzniveau gewährleistet ist (Entscheidung 2002/2/EG vom 20. Dezember 2001).

Eine andere Lösung hat die Europäische Union für Datentransfers in die USA erarbeitet. Das Datenschutzniveau in den USA kann grundsätzlich nicht als angemessen angesehen werden. Von der Europäischen Union wurden aber so genannte "Grundsätze des Sicheren Hafens" mit dem amerikanischen Handelsministerium vereinbart. Amerikanische Unternehmen können diesen Grundsätzen, die allgemein auch als **Safe Harbor Abkommen** bezeichnet werden, beitreten. Für dem Abkommen beigetretene Unternehmen hat die EU-Kommission mit ihrer Entscheidung vom 26. Juli 2000 (2000/520/EG) festgestellt, dass bei diesen Unternehmen von einem angemessenen Datenschutzniveau ausgegangen werden kann.

Die Liste der dem Safe Harbor Abkommen beigetretenen US-Unternehmen kann unter www.export.gov/safeharbor abgerufen werden. Die in diesem Abschnitt angesprochenen Entscheidungen der Kommission sind unter der Internetadresse www.europa.eu.int zu finden.

Bietet eine Stelle in einem Drittstaat hingegen **kein angemessenes Datenschutzniveau**, ist eine Datenübermittlung, die materiell datenschutzrechtlich zulässig ist, an eine solche Stelle nur möglich, wenn

- ein in § 4c Abs. 1 BDSG genannter Ausnahmetatbestand vorliegt

  oder

- zwischen der datenübermittelnden und der datenempfangenden Stelle ein von der EU-Kommission empfohlener Standardvertrag abgeschlossen wurde. Die Kommission hat in ihren Entscheidungen vom 15. Juni 2001 (2001/497/EG) und 27. Dezember 2001 (2002/16/EG), abrufbar unter www.europa.eu.int, **Standardvertragsklauseln** entwickelt, mit denen die am Datentransfer beteiligten Stellen **Garantien für die Persönlichkeitsrechte** der von der Übermittlung Betroffenen geben. Die Entscheidung aus Juni 2001 bezieht sich auf die Übermittlung von Daten zwischen zwei verantwortlichen Stellen, die Entscheidung aus Dezember 2001 enthält einen Standardvertrag speziell für die Datenübermittlung an einen in einem Drittstaat ansässigen Auftragsdatenverarbeiter. Aus § 3 Abs. 8 i.V.m. § 3 Abs. 4 Nr. 3 BDSG ergibt sich, dass auch der Datentransfer zwischen Auftraggeber und Auftragnehmer als Übermittlung - nicht als Auftragsdatenverarbeitung - zu behandeln ist, wenn der Auftragnehmer in einem Drittstaat ansässig ist.

- Wird ein Datentransfer in einen Drittstaat unter wortgetreuer Verwendung von Standardvertragsklauseln vorgenommen, bedarf es keiner Genehmigung der Aufsichtsbehörde nach § 4c Abs. 2 BDSG. Die Kommissionsentscheidungen stehen als supranationale Rechtsetzungsakte selbstständig neben den Regelungen des BDSG für die Datenübermittlung in das Ausland.

- Schließlich können Garantien für die Persönlichkeitsrechte der von Datenübermittlungen in einen Drittstaat Betroffenen auch in einem **Individualvertrag** zwischen der übermittelnden und der empfangenden Stelle oder - bei Übermittlungen zwischen konzernan-

gehörigen Unternehmen - **in verbindlichen konzerninternen Unternehmensregelungen** gegeben werden. Sollen solche individuellen Regelungen Basis für einen Datentransfer in einen Drittstaat sein, ist vor der Datenübermittlung die Genehmigung der Aufsichtsbehörde gemäß § 4c Abs. 2 BDSG einzuholen. Die Aufsichtsbehörde prüft, ob die in der Regelung enthaltenen Garantien dem Schutz des Persönlichkeitsrechts der Betroffenen ausreichend Rechnung tragen.

5 Videoüberwachung

Die rasche Weiterentwicklung der Videotechnik (beispielsweise Gesichtserkennungssysteme) ist ebenso Besorgnis erregend wie die **stetige Zunahme** der Anwendung in vielen Bereichen des täglichen Lebens. Mit dem Einsatz dieser Technik sind Eingriffe in das Recht der Betroffenen auf informationelle Selbstbestimmung und in ihr allgemeines Persönlichkeitsrecht verbunden, die mit den Mitteln der Aufsichtsbehörde im nicht-öffentlichen Bereich oft nicht in dem wünschenswerten Maße nachprüfbar sind.

Seit dem letzten Datenschutzbericht (15. Datenschutzbericht 2001 unter 3., S. 60) hat sich die Rechtslage geändert. Im öffentlichen Bereich sind die Befugnisse der Polizei erweitert worden. Im nicht-öffentlichen Bereich ist nunmehr die Zulässigkeit der Videoüberwachung nach der speziellen Vorschrift des § 6b BDSG zu prüfen. In diesem Bereich hat besonders die Einrichtung von Videoüberwachung in öffentlichen Verkehrsmitteln, an Haltestellen und Bahnhöfen zugenommen. Außerdem erfreuen sich nachbarliche Überwachungskameras bei privaten Grundstückseigentümerinnen und -eigentümern sowie Webcams, mit denen private Personen Bildaufnahmen ins Internet stellen, leider immer größerer Beliebtheit.

Mit der geplanten Änderung des nordrhein-westfälischen **Polizeigesetzes** (PolG NRW) ist beabsichtigt, die strengen Voraussetzungen für einen **Videoeinsatz an öffentlichen Straßen und Plätzen** zu lockern und damit die Möglichkeiten der Videoüberwachung einzelner öffentlich zugänglicher Orte erheblich zu erleichtern. Wenn auch mit nahezu flächendeckenden Überwachungen von Straßenzügen oder gar Stadtvierteln und mithin „britischen Verhältnissen" noch nicht zu rechnen ist, muss die mit der geplanten Neufassung eintretende **Senkung der Einsatzschwelle** für Videoüberwachungen als weiterer Schritt in diese Richtung angesehen werden. Straftaten von „erheblicher Bedeutung" sollen künftig nicht mehr erforderlich sein, um solche Überwachungen durchführen zu können. Auch sollen die Aufzeichnungsmöglichkeiten sehr erweitert werden. Datenschutzrechtliche Bedenken gegen den Gesetzentwurf blieben bisher leider unberücksichtigt. Nach wie vor ist im Übrigen nicht belegt, dass eine Videoüberwachung zu der behaupteten Reduzierung von Straftaten führt und nicht nur eine bloße Verdrängung bewirkt.

Jeder Einsatz von **Videoüberwachung im nicht-öffentlichen Bereich** - durch private Personen oder Unternehmen - ist jetzt nach den Voraussetzungen der spezialgesetzlichen Regelung in **§ 6b BDSG** zu prüfen. Allerdings erfasst die Regelung nur die Überwachung öffentlich zugänglicher Räume. Es fehlen somit besondere Schutzvorschriften für die Fälle der Überwachung sensibler Bereiche wie Arbeitsplätze und Wohnhäuser. Problematisch ist auch die Regelung in § 6b Abs. 1 Nr. 3 BDSG, weil hier eine Zulassung von Videoüberwachung zur Wahrnehmung berechtigter Interessen als generelle Auffangregelung verstanden wird, die aber nach den Grundsätzen des Datenschutzes allenfalls in extremen Ausnahmefällen in Frage kommen könnte. Bisher ist kein Fall bekannt geworden, in welchem eine Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret bestimmte Zwecke erforderlich sein sollte.

Zum Einsatz von **Videoüberwachung in öffentlichen Verkehrsmitteln** (15. Datenschutzbericht 2001 unter 3.2.3, S. 69) sind inzwischen die Anforderungen an eine zulässige Überwachung in Bahnen, Straßenbahnen und Bussen der Verkehrsunternehmen bundesweit erörtert, abgestimmt und verabschiedet worden. An der Erarbeitung der Kriterien waren der Verband Deutscher Verkehrsunternehmen in Köln und dessen Gremien, die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beteiligt. Damit sind die festgelegten Kriterien grundsätzlich bundesweit Maßstab für die Prüfung der datenschutzrechtlichen Zulässigkeit. Die Anforderungen sind im Anhang unter Nr. 6 abgedruckt. In Nordrhein-Westfalen werden Fördermittel für Sicherheitseinrichtungen - auch für Videoüberwachungsanlagen - in Verkehrsmitteln gewährt. Um zu verhindern, dass etwa datenschutzrechtlich unzulässige Überwachungseinrichtungen geplant und bezuschusst werden, wurde das Verkehrsministerium gebeten, den Anforderungskatalog an die Bewilligungsbehörden weiterzuleiten und die Zuwendungsempfängerinnen und -empfänger zu verpflichten, in dem mit dem Bewilligungsantrag vorzulegenden Sicherheitskonzept auch die datenschutzrechtlichen Anforderungen zu berücksichtigen.

Aus dem privaten Bereich kommen häufig Beschwerden von Grundstückseigentümerinnen und -eigentümern, deren Grundstücke durch die Videokameras ihrer **Nachbarinnen und Nachbarn** beobachtet werden. Solche Beobachtungen sind **in der Regel unzulässig**, weil sie nicht mehr zur Wahrnehmung des **Hausrechts** erfolgen, das heißt zur Abwehr von

Gefahren für die Sicherheit der im Haus lebenden Personen oder für ihr Eigentum. Außerdem werden die schutzwürdigen Interessen der Betroffenen erheblich beeinträchtigt. In manchen Fällen sind die Videokameras sogar so eingestellt, dass sie über das eigene Grundstück hinaus nicht nur auf das Nachbargrundstück, sondern gleich noch in den öffentlichen Verkehrsraum hinein Beobachtungen ermöglichen. Die Zulässigkeit einer Beobachtung endet an der eigenen Grundstücksgrenze, weil schon das Hausrecht nicht weiter reicht.

Selbst innerhalb von privaten **Wohngebäuden** wird zunehmend Videoüberwachung eingesetzt, um etwa die Beschädigung von Aufzügen oder Briefkästen zu verhindern. Die Zulässigkeit einer solchen Videoüberwachung ist nicht nach § 6b BDSG zu beurteilen, weil sie in einem **nicht öffentlich zugänglichen Raum** stattfindet. Dennoch wird auch hier durch die installierten Kameras das allgemeine Persönlichkeitsrecht der Mieterinnen und Mieter sowie der Besucherinnen und Besucher beeinträchtigt. Das allgemeine Persönlichkeitsrecht ist nicht nur vom Staat, sondern aufgrund seiner Ausstrahlungswirkung auch im Privatrechtsverkehr zu beachten. Mieterinnen und Mieter haben das Recht, sich im Haus prinzipiell unbeobachtet bewegen zu können. Im Rahmen des Mietverhältnisses dürfen grundsätzlich nur diejenigen Daten der Mietparteien verarbeitet werden, die aus mietrechtlichen Gründen erforderlich sind (§ 28 Abs. 1 Nr. 1 BDSG). Andere Daten dürfen nur zur Wahrung berechtigter Interessen verarbeitet werden. Und dies darf auch nur dann geschehen, wenn kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Mieterinnen und Mieter am Ausschluss einer Videoüberwachung überwiegen (§ 28 Abs. 1 Nr. 2 BDSG). Dies ist vor allem dann zu prüfen, wenn die Videoüberwachung zur Wahrung des Hausrechts nicht erforderlich ist und schutzwürdige Interessen der Mieterinnen und Mieter beeinträchtigt werden. Also entsprechen diese Voraussetzungen denen des § 6b BDSG.

Beispielsweise hatte die Hausverwaltung einer Wohnanlage im Hauseingangsbereich zwei Videokameras installiert, die auf die Briefkästen und eine Aufenthaltsecke ausgerichtet waren. Während die Videokamera zur Überwachung einer **Briefkastenanlage** zulässig ist, konnte dies für die auf die **Aufenthaltsecke im Eingangsbereich** gerichtete Kamera nicht gelten. In der Vergangenheit wurden immer wieder einzelne Briefkästen beschädigt und Post entwendet. Außerdem überwiegen die schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen in diesem Fall nicht

die Interessen des Eigentumsschutzes. Sie entsprechen vielmehr auch den Interessen der Mietparteien an einer ordnungsgemäßen Postzustellung. Die Überwachung erfolgt hier gerade auch zum Schutz der Hausbewohnerinnen und Hausbewohner. Darüber hinaus wird der Bereich der Briefkästen nur kurzfristig betreten, und eine Beobachtung der entnommenen Post ist nicht möglich. Allerdings musste ein deutlich erkennbares **Piktogramm** in unmittelbarer Nähe der Briefkastenanlage angebracht werden, das auf die Videoüberwachung hinweist. Die andere auf die Aufenthaltsecke gerichtete Kamera war dagegen zur Wahrnehmung des Hausrechts nicht erforderlich, da die Vorkommnisse (Entzünden eines Papierkorbes und Beschädigung einer Glasscheibe) bereits über zwei Jahre zurücklagen.

Die technischen Möglichkeiten einer Kombination von Videoüberwachung mit Gesichtserkennungssystemen stellen wiederum neue Anforderungen an den Datenschutz. Neue Technik wird zunächst eingesetzt, ohne ihre Vereinbarkeit mit datenschutzrechtlichen Grundsätzen zu prüfen. Sowohl im öffentlichen wie auch im privaten Bereich ist aus Gründen des Datenschutzes vor einem Einsatz neuer Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten zu prüfen, ob das geplante Verfahren besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist (§ 4d Abs. 5 BDSG) oder ob durch den Einsatz eines automatisierten Verfahrens Gefahren für das Recht auf informationelle Selbstbestimmung entstehen (§ 10 Abs. 3 Satz 1 DSG NRW). Der Einsatz von **Gesichtserkennungssystemen** mit den damit installierten automatisierten Verfahren bewirkt grundsätzlich gegenüber „bloßer" Videoüberwachung **zusätzliche Eingriffe** in die Rechte der Betroffenen mit einer neuen Eingriffstiefe. Zur Funktion eines Gesichtserkennungssystems gehört häufig der Aufbau und die Pflege einer Bilddatenbank und der Abgleich neu gewonnener mit den in der Datenbank gespeicherten Bildern sowie die automatische Speicherung neuer Aufnahmen. Ob solche Verfahren in Kombination mit der Videoüberwachung noch von den rechtlichen Zulässigkeitsvoraussetzungen des § 6b BDSG oder etwa §§ 15a PolG NRW, 29b DSG NRW umfasst sind, muss erheblich bezweifelt werden. Es bedarf vielmehr einer **speziellen gesetzlichen Regelung**, die notwendige Anforderungen an einen zulässigen Einsatz für einen bestimmten Bereich festlegt. Solange eine solche gesetzliche Regelung fehlt, darf ihre Einführung nicht auf allgemeine Datenschutzvorschriften gestützt werden.

Zum Schluss muss noch die leider um sich greifende „Unsitte" von Internetfreaks erwähnt werden, die ihre Umgebung mit Hilfe einer Webcam auf der eigenen Website abbilden und zwar so, dass auch **Personen erkennbar** sind. In nahezu allen Fällen geschieht dies zur Eigenwerbung oder Selbstdarstellung. Unabhängig davon, dass hierfür kein nach § 6b BDSG berechtigtes Interesse besteht, ist es darüber hinaus nicht erforderlich, personenscharfe Aufnahmen - also Aufnahmen, auf denen Personen identifiziert werden können - im Internet weltweit zu veröffentlichen. Übersichtsaufnahmen reichen vollkommen aus.

6 Wohnen und Liegenschaften

6.1 Warndatei im Wohnungswesen

Ein neues Geschäftsfeld im Internet sind Auskunfteien, in denen zum Beispiel Informationen über „auffällige" Mieterinnen und Mieter gesammelt und von Vermieterinnen und Vermietern abgerufen werden können. Gegen solche Warndateien bestehen grundsätzliche datenschutzrechtliche Bedenken.

Grundsätzlich ist die Errichtung einer Warndatei für die angeschlossenen Vertragspartnerinnen und Vertragspartner unter Beachtung des § 29 BDSG **unzulässig**. Abfragbare Informationen über Mieterinnen und Mieter dürfen weder erhoben noch zum Zweck der Übermittlung gespeichert werden, wenn deren schutzwürdige Interessen als Wohnungssuchende zu berücksichtigen sind. Denn selbst bei optimaler Wohnungsmarktsituation kann die Verweigerung des Abschlusses eines Mietvertrages schwere Nachteile bewirken. Wohnraum gehört zu den Grundbedürfnissen des Menschen. Die Nichtgewährung von Wohnraum bewirkt viel schwerer wiegende Folgen als etwa die Verweigerung eines Kredits oder die Ablehnung eines weiteren Kaufvertrages mit Ratenzahlung.

Dennoch können **ausnahmsweise berechtigte Interessen** auf Seiten der Vermieterinnen und Vermieter bestehen, vor Entscheidung über den Abschluss eines Mietvertrages Informationen über die Zuverlässigkeit der Mietpartei einzuholen. Berechtigte Interessen liegen in dem legitimen Schutz des Eigentums, in dem Bestreben, Wohnraum verfügbar zu halten und in der Bewahrung eines friedvollen Zusammenlebens in einem Wohngebäude.

Auch wenn es bei berechtigtem Interesse der Vermieterinnen und Vermieter nützlich und erstrebenswert sein könnte, möglichst viele Informationen über die Bonität von Mieterinnen und Mietern aus einer Warndatei abrufen zu können, wäre die Einrichtung einer **umfassenden Datei** dennoch aus Gründen des Schutzes der Betroffenen **unzulässig**. Die Aufnahme von Negativdaten in einer Warndatei kann wegen der **schutzwürdigen Interessen** der Mieterinnen und Mieter nur eingeschränkt zulässig sein. In Betracht kommen dabei nur Informationen, die auf von der Rechtsordnung gebilligten mietrechtlichen Entscheidungen beruhen (vgl. § 543 Bürgerliches Gesetzbuch). Handelt es sich nämlich um solche Angaben, fallen entweder keine schutzwürdigen Interessen von Mietparteien ins Gewicht oder sie müssen

ausnahmsweise hinter die berechtigten Interessen der Wohnungseigentümerinnen und Wohnungseigentümer zurücktreten.

Vor diesem Hintergrund müssen die Informationen, die in eine solche Warndatei eingemeldet werden können und über die Auskunft erteilt werden darf, nach Art, Inhalt und Aussagekraft objektiv feststellbar, sachlich richtig und den Zwecken angemessen sein. Wegen der negativen Auswirkungen, die eine Übermittlung entsprechender Daten an Vermieterinnen und Vermieter oder Wohnungsgesellschaften für die betroffene Person haben kann, müssen außerdem Anforderungen an die Datenverarbeitung beachtet und Garantien abgegeben werden, die die legitimen Rechte der Betroffenen wahren.

Aus diesen Gründen dürfen in eine Warndatei allenfalls folgende **objektive Negativmerkmale** aufgenommen werden:

- rechtskräftiges Urteil zur fristlosen Kündigung wegen Zahlungsverzug,
- rechtskräftiges Urteil zur fristlosen Kündigung wegen vertragswidrigen Verhaltens,
- rechtskräftiges Räumungsurteil,
- Vollstreckungsbescheid wegen Mietschulden (mindestens in Höhe zweier Monatsmieten einschließlich Nebenkosten),
- von der Gerichtsvollzieherin oder dem Gerichtsvollzieher bescheinigte fruchtlose Pfändung einer titulierten Forderung aus dem Mietverhältnis (Forderung mindestens in vergleichbarer Höhe) oder die von einer Vermieterin oder einem Vermieter erwirkte Abgabe einer eidesstattlichen Versicherung oder eines Haftbefehls.

Darüber hinaus ist ein **Merkblatt** mit Informationen erforderlich, das den Mieterinnen und Mietern vor Abschluss des Mietvertrages ausgehändigt werden muss. Hierin sind sie insbesondere über die Abfrage- und Einmeldemöglichkeit der Vermieterin oder des Vermieters ausführlich zu unterrichten. Außerdem besteht unter anderem die Pflicht, einen **Eintrag** in eine Warndatei am Ende des dritten Kalenderjahres zu **löschen** und den unentgeltlichen Auskunfts- und Widerspruchsrechten der Betroffenen nach §§ 34 Abs. 5 und § 35 Abs. 5 BDSG Rechnung zu tragen.

Ein automatisiertes Abrufverfahren darf nur für Vertragspartnerinnen und -partner zugelassen werden, bei denen dies wegen der Vielzahl der

Übermittlungen oder der Eilbedürftigkeit angemessen ist. Dann müssen die Abrufe vom Unternehmen aber auch zu **Kontrollzwecken protokolliert** werden. Unzulässige Zugriffe führen zu einem Ausschluss vom Abrufverfahren. Schließlich müssen sich die Vertragspartnerinnen und -partner dazu verpflichten, die betroffene Mietpartei über jede Einmeldung zu unterrichten. Abfragen nur im Falle eines Mietvertragsabschlusses vorzunehmen und eine mietvertragliche Entscheidung nicht allein auf die Erkenntnisse aus der Warndatei zu stützen. Sie dürfen die abgefragten Daten nur für eigene Zwecke verwenden und müssen sie nach Ablauf des dritten Kalenderjahres oder nach Beendigung des Mietverhältnisses selbst auch löschen. Damit soll eine datenschutzrechtlich hinnehmbare Nutzung der Warndatei sichergestellt werden.

Nur dann, wenn alle genannten Anforderungen beachtet werden, bestehen keine durchgreifenden datenschutzrechtlichen Bedenken gegen die Errichtung einer Warndatei im Wohnungswesen. Auch die anderen in diesem Bereich tätigen Auskunfteien müssen an diesen Maßstäben gemessen werden.

6.2 Mietbewerbungsbogen und Selbstauskünfte

„Wohnung oder Weitersuche?" - Das ist oft die Frage, wenn sich potentielle Mieterinnen und Mieter vor dem Abschluss eines Mietvertrages entscheiden müssen, entweder einen Bewerbungsbogen mit detaillierten persönlichen Fragen zu beantworten oder auf die Wohnung zu verzichten.

Große Wohnungsgesellschaften wie auch Vermieterinnen und Vermieter einzelner Wohneinheiten verlangen häufig die Angabe personenbezogener Daten in einem **Mietbewerbungsbogen** oder gar die Vorlage einer **Selbstauskunft.** Dies kann eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts der betroffenen Personen bewirken. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Zulässig ist diese Datenerhebung nach Maßgabe des § 28 Abs. 1 BDSG, wenn sie für den Abschluss eines **Mietvertrages erforderlich** ist, das heißt, wenn sie geeignet und notwendig ist, eine Entscheidung der Vermieterin oder des Vermieters über den Abschluss des Mietvertrages herbeizuführen.

Als zulässig wird zum Beispiel die Erhebung folgender Angaben erachtet: Name und Vorname, Geburtsdatum, Anschrift, private Telefonnummer, feste Anstellung (ja nein), ungefähre Einkommensverhältnisse, Eidesstattliche Versicherung abgegeben (ja nein), ergangener Räumungstitel (ja nein) und erfolgte Einstweilige Verfügung in Mietsachen. Nicht ersichtlich ist dagegen, dass beispielsweise Angaben über Nationalität oder Staatsangehörigkeit, Personalausweisnummer, Anschrift der Arbeitgeberin oder des Arbeitgebers und Beschäftigungsdauer, Anschrift der Vorvermieterin oder des Vorvermieters, Pkw-Kennzeichen, Bankverbindung, generelle Fragen nach Schulden und Unterhaltsverpflichtungen für den beabsichtigten Zweck erforderlich sind, nämlich für die Entscheidung über den Abschluss eines Mietvertrages. Die Erhebung solcher Angaben ist deshalb **unzulässig**.

Im Vorspann zu Bewerbungsbögen müssen die Mieterinnen und Mieter in geeigneter Weise darüber **unterrichtet** werden, dass die erhobenen Daten im Zusammenhang mit der Bearbeitung der Bewerbung und dem Führen eines Mietkontos gespeichert und verarbeitet werden. Außerdem müssen die Bewerbungsbögen **vernichtet** werden, wenn kein Mietvertrag zustande kommt.

Sollte beabsichtigt sein, Auskünfte bei Dritten (zum Beispiel Vorvermieterinnen und -vermietern oder am Arbeitsplatz) zu erfragen, so ist dies nur zulässig, wenn eine wirksame **Einwilligung** der betroffenen Person eingeholt wurde.

Erhebliche datenschutzrechtliche Bedenken bestehen überdies, wenn Vermieterinnen oder Vermieter neben dem Ausfüllen eines Mietbewerbungsbogens außerdem noch die Vorlage einer **Selbstauskunft** verlangen, die von den Betroffenen bei den großen Auskunfteien selbst besorgt werden müssen. Diese so genannten Selbstauskünfte enthalten wesentlich **mehr Angaben** über die finanziellen Verhältnisse der Betroffenen als etwa die Vermieterin oder der Vermieter über die Einholung einer Auskunft als Vertragspartnerin oder -partner der Auskunftei selbst (beispielsweise Schufa oder Creditreform) bekommen würden. Meist wird die Zulässigkeit, Selbstauskünfte einzuholen, auf die Einwilligung der Betroffenen gestützt. Eine Einwilligung wäre jedoch nur wirksam, wenn sie freiwillig erteilt würde. Die Betroffenen befinden sich jedoch in einer Zwangssituation, so dass es an der erforderlichen Freiwilligkeit und damit an der Wirksamkeit der Einwilligung fehlt.

Mietbewerbungsbögen enthalten oft unzulässige Fragen. Selbstauskünfte dürfen von Vermieterinnen und Vermietern nicht verlangt werden.

6.3 Geobasisdaten - Informationssysteme offen für kommerzielle Nutzung?

Die kommerzielle Nutzung von ortsbezogenen Grundstücks- und Gebäudedaten aus den öffentlichen Vermessungs- und Liegenschaftskatastern wird zielstrebig weiter entwickelt. Dieser Nutzung stehen Befürchtungen der Grundstückseigentümerinnen und -eigentümer bezüglich der Preisgabe ihrer Daten gegenüber.

Geobasisdaten sind im öffentlichen Bereich wesentlicher Bestandteil von digitalen Liegenschaftskarten, elektronischen Grundbucheintragungen, digitalen Luftbildkarten und Bodeninformationssystemen, um nur einige Verfahren der neuen Informationstechniken zu nennen. Der zunehmende Einsatz dieser Techniken bringt zwangsläufig Veränderungen im Umgang auch mit personenbezogenen Daten mit sich. Soweit einschränkende Vorschriften einem allgemeinen Zugang und einer kommerziellen Nutzung entgegen stehen, werden rechtliche Anpassungen notwendig (beispielsweise im Vermessungs- und Katastergesetz sowie in der Katasterdatenübermittlungsverordnung), damit keine Wertungswidersprüche auftreten. Gegen solche gesetzlichen Anpassungen bestehen solange keine Bedenken, wie den Anforderungen zum **Schutz der Persönlichkeitsrechte** der Betroffenen auch bei Einsatz neuer Verfahren und Techniken im erforderlichen Umfang Rechnung getragen wird.

Das Landesvermessungsamt vertreibt Geobasisdaten etwa in Form der digitalen Grundkarte an die Kreise und kreisfreien Städte als Katasterbehörden und an Dritte zur kommerziellen Verwendung. Über Angebot und Nutzungsmöglichkeiten der Produkte der Landesvermessung wird die Öffentlichkeit informiert. Zu öffentlichen Zwecken gewonnene Geobasisdaten sollen den Bedürfnissen unter anderem auch der Wirtschaft und des Verkehrs entsprechen. Daneben werden in einem nordrhein-westfälischen Pilotprojekt digitale Liegenschaftskarten einem Nutzerkreis online zugänglich gemacht. Nach besonderen Verträgen, die von ausgewählten Katasterämtern geschlossen werden, sind Abrufe von Sachdaten und Daten der Grundstückseigentümerinnen und -eigentümer sowie von Nutzungsberechtigten möglich. Dabei wird das berechtigte Interesse der Vertragspartnerinnen und -partner leider immer oberflächlicher

geprüft, weil diese Prüfung im Online-Verfahren auf wenige vorgegebene Gründe beschränkt ist. Deshalb stellt sich zunehmend die Frage, wie mit der **Offenbarung personenbeziehbarer Daten** (von Grundstückseigentümerinnen und -eigentümern oder Nutzungsberechtigten) in kartografischen Darstellungen in kleinem Maßstab (etwa 1:5000) oder in digitalen Luftbildern zusammen mit Geokoordinaten und entsprechenden Straßenverzeichnissen umgegangen werden soll. Diese Geobasisdaten sind personenbeziehbar und lassen unvermeidlich auch verschiedene Aussagen über Grundstücke und darauf stehenden Gebäuden zu. Sie werden bereits heute in andere Datenbanken exportiert und dort mit neuen Aussagen verknüpft, weil sie nur so für unterschiedliche wirtschaftliche Interessen verwertbar sind. Deshalb muss der Gesetzgeber Klarheit über den praktisch sehr weiten Informationszugang zu solchen personenbeziehbaren Daten schaffen. Eine sonst notwendige Darstellung von Geobasisdaten etwa unter Ausblendung von personenbezogenen kartografischen Darstellungen dürfte schlechterdings praxisfremd sein.

Parallel dazu sind auch im nicht-öffentlichen Bereich Informationssysteme mit multifunktionaler Anwendung entwickelt worden, die im Wesentlichen auf den gleichen Geobasisdaten aufbauen. Teils sind diese Daten von öffentlichen Stellen übernommen, teils von den Unternehmen durch eigene Luftbildflüge und öffentlich zugängliche Straßenverzeichnisse (in NRW über das Informationsfreiheitsgesetz - IFG NRW) oder Adressdatenbanken selbst erhoben worden. Geprägt ist die **kommerzielle Nutzung** immer durch den Personenbezug zu den Geobasisdaten und deren Verknüpfung mit Daten aus anderen Datenbanken - meist der großen Auskunfteien (etwa zur Bonitätsprüfung oder Vertragskontrolle). Damit erfolgt eine zweckändernde Nutzung, deren Zulässigkeit gesondert zu prüfen ist.

In jedem Einzelfall ist zu prüfen, ob die jeweilige Nutzung und Verknüpfung von Daten aus anderen Datenbanken mit den Geobasisdaten und ihre Verwendung zu neuen Geschäftszwecken zulässig ist.

6.4 Luftbildaufnahmen von Gebäuden und Grundstücken

Häufig wurde im Berichtszeitraum die Frage gestellt, ob es gegen den Datenschutz verstößt, wenn von Gebäuden oder Grundstücken Luftbildaufnahmen gefertigt werden.

Unternehmen, die Luftbildaufnahmen gewerblich herstellen und nutzen, verfolgen mehrere Geschäftsziele: Die in Massen hergestellten Luftbildaufnahmen einzelner Gebäude und Grundstücke werden entweder Grundstückseigentümerinnen und -eigentümern oder Nutzungsberechtigten zum Kauf angeboten. Oder es werden großflächige Luftbildaufnahmen für Planungszwecke oder für die Erstellung von Luftbildkarten genutzt. Im zweiten Fall ist das Luftbildunternehmen nach § 2 Abs. 5 Vermessungs- und Katastergesetz NRW verpflichtet, die dafür durchzuführenden Bildflüge dem Landesvermessungsamt anzuzeigen und das dabei gewonnene Bildmaterial zur Verfügung zu stellen. Schließlich werden zunehmend digitale Luftbilder in Datenbanken mit genauen Lagebezeichnungen eingespeist und einem Kreis von Vertragspartnerinnen und -partnern online zur Verfügung gestellt.

Soweit die Bilder den Betroffenen zum Kauf angeboten, ausschließlich für diesen Geschäftszweck gespeichert sowie genutzt und bei Erreichen (Kauf) oder endgültigem Verfehlen (Nichtkauf) dieses Zwecks bei dem Unternehmen gelöscht werden, bestehen keine datenschutzrechtlichen Bedenken.

Ansonsten ist eine **differenzierte Betrachtung** geboten. In der Regel werden bei Luftbildaufnahmen grundstücks- oder gebäudebezogene Daten gespeichert, die allgemein zugänglich sind (vgl. Urteil des OLG Karlsruhe vom 16. März 2000 - 4 U 145/99 - 1 O 200/99). Allgemein zugängliche Daten sind dann nicht besonders zu schützen, wenn die den Bildern zu entnehmenden Angaben **aus sich heraus nicht personenbeziehbar** sind. Das ist dann der Fall, wenn ein Personenbezug nur durch Einsichtnahme in das Grundbuch oder die Liegenschaftskarte - und dort nur bei berechtigtem Interesse - hergestellt werden kann. Einer weiteren Datenverarbeitung ohne Angaben zur Person - etwa eines luftbildbasierten Stadtplanes - stehen grundsätzlich keine überwiegenden schutzwürdigen Interessen der Grundstückseigentümerinnen und -eigentümer entgegen, so dass einer solchen Datenverarbeitung nach Maßgabe des § 29 BDSG keine datenschutzrechtlichen Bedenken begegnen.

Anders verhält es sich, wenn die digitalen Luftbilder **online** abgerufen, **verändert** (durch Zoomen) und mit anderen Dateien **verknüpft** werden können, beispielsweise mit einer Datenbank, die Daten über wirtschaftliche oder finanzielle Verhältnisse von Grundstückseigentümerinnen und -eigentümern oder Nutzungsberechtigten enthält. In solchen Fällen muss von einem **überwiegenden schutzwürdigen Interesse** der betroffenen

Personen ausgegangen werden. Die Speicherung, Verarbeitung und Nutzung dieser Daten ist unzulässig, es sei denn, die Betroffenen willigen in die Nutzung ihrer Daten ein.

Datenschutzrechtlich unbedenklich ist der Fall eines kommerziellen Online-Dienstes für Dachdeckerbetriebe, mit dessen Hilfe Betriebe aus den abrufbaren Luftbildkarten erst durch Eingabe von Straße und Hausnummer ein bestimmtes Gebäude von oben dargestellt erhalten und so dessen Dachmaße berechnen können. Dies setzt voraus, dass diejenige Person, der das Grundstück gehört, als Auftraggeberin dem Dachdeckerbetrieb die **Einwilligung** erteilt hat, zur Erstellung eines Kostenvoranschlages oder zur Durchführung und Abrechnung der Dachdeckerarbeiten die benötigten Daten ihres Gebäudes abzurufen und zu speichern.

Demgegenüber gibt es Unternehmen, die ihren Vertragspartnerinnen und -partnern (zum Beispiel Versorgungsunternehmen, Architektenbüros, Banken und Versicherungen) zusammen mit digitalen Luftbildern weitere Daten liefern. Vor allem können dies bereits **geocodierte Gebäudedaten** sein, die aus der unternehmenseigenen Gebäudedatenbank abgerufen werden. In ihr sind hausgenaue Geokoordinaten enthalten, die eine genaue Entschlüsselung in Straße, Hausnummer, Hausnummerzusatz, Postleitzahl, Ort und Ortsteil zulassen. Ohne diese Angaben wären sie für die Vertragspartnerinnen und -partner nicht nutzbar. Das Unternehmen ist zwar der Auffassung, nur Sachdaten vorzuhalten, die keine Verknüpfung zu Personendaten zulassen. Nach § 3 Abs. 1 BDSG sind die Daten aber personenbeziehbar. Allerdings dürfen nach § 29 Abs. 1 Nr. 2 BDSG geocodierte Gebäudedaten als allgemein zugängliche Daten gewerbsmäßig gespeichert und übermittelt werden, wenn schutzwürdige Interessen von betroffenen Grundstückseigentümerinnen und -eigentümern nicht offensichtlich überwiegen. Kommen die gegebenen Informationen über eine **„Stadtplanqualität"** nicht hinaus, greifen sie nicht wesentlich in die Persönlichkeitsrechte der Betroffenen ein. Problematisch können dagegen Abruf und Nutzung von Grundstücks- und Gebäudedaten sein, die mit **sensiblen Angaben** über die Bonität der Eigentümerin oder des Eigentümers oder etwa mit Hinweisen auf eingeschränkte Nutzungsmöglichkeiten durch Bodenbelastungen oder bauplanerische Einschränkungen verknüpft sind.

Bei geocodierten Gebäudedaten kommt es darauf an, dass einer Verknüpfung oder Nutzung derart übermittelter Daten schutzwürdige

Interessen der betroffenen Personen (§ 29 Abs. 1 Nr. 1 BDSG) nicht entgegen stehen.

6.5 Denkmalliste im Internet

Dürfen Informationen über Bau- und Bodendenkmäler im Internet veröffentlicht werden, wenn ihre Lagen mit Straßennamen und Hausnummern oder mit den Grundbuchbezeichnungen genau angegeben sind und so Rückschlüsse auf die Grundstückseigentümerinnen und -eigentümer möglich sind?

Datenschutzrechtlich relevant sind alle Eintragungen in der Liste, soweit sie sich auf Grundstücke beziehen, die im Eigentum **natürlicher Personen** stehen. Selbst wenn in der Liste keine Namen der Nutzungsberechtigten oder Eigentümerinnen und Eigentümer erscheinen, geben die eingetragenen Daten Auskunft über sachliche Verhältnisse einer bestimmbaren Person, nämlich dass sich auf dem genau bezeichneten Grundstück dieser Person ein Denkmal befindet. Es ist dabei unerheblich, dass der Bezug zur natürlichen Person erst über die Liegenschaftskarte oder das Grundbuch hergestellt werden kann, weil bereits das berechtigte Interesse einer dritten Person, die beispielsweise mit Immobilien makelt, ausreicht, um Zugang zu diesen Daten zu erhalten. Daher sind alle Angaben in der Denkmalliste über Grundstücke natürlicher Personen vom Datenschutz umfasst.

Die datenschutzrechtliche Relevanz der Informationen bedeutet allerdings nicht, dass ihre Veröffentlichung im Internet deshalb bereits automatisch unzulässig wäre. Es fragt sich, ob der Schutz der personenbezogenen (Grundstücks-) Daten hinter das öffentliche Interesse an einer Veröffentlichung von unter Denkmalschutz gestellten Bau- und Bodenobjekten zurücktreten muss. Hierfür spricht die Regelung des § 3 Abs. 5 Denkmalschutzgesetz NRW, wonach jede Person **Einblick** in die **Denkmalliste** nehmen kann. Allerdings ermöglicht diese Einsichtnahme jeder informationssuchenden Person lediglich, die Eintragungen auf den Karteikarten der kommunalen Denkmalämter zu lesen. Würden die Angaben dagegen im Internet veröffentlicht, wären sie jederzeit weltweit elektronisch einseh- und abrufbar; heruntergeladene Daten über Grundstücke könnten überdies mit anderen kommerziellen oder sonstigen Datenbeständen verknüpft werden. Daher bestanden vor dem In-Kraft-Treten des **Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW)** im Januar 2002 Bedenken gegen eine Veröffentlichung von Denkmallisten im Internet.

Durch das In-Kraft-Treten des IFG NRW hat sich die Rechtslage indes geändert. Zwar sind auch nach diesem Gesetz grundsätzlich alle personenbezogenen Daten geschützt, aber es bestehen Ausnahmen, die auch den Zugang zu personenbezogenen Daten eröffnen können. Nach § 9 Abs. 1 Buchstabe b) IFG NRW ist dies der Fall, wenn eine Rechtsvorschrift die Bekanntgabe personenbezogener Daten erlaubt. Eine solche Erlaubnis ist in § 3 Abs. 5 Satz 1 Denkmalschutzgesetz festgeschrieben. Die **zulässige Veröffentlichung** kann im Sinne des § 12 Satz 3 IFG NRW auch in elektronischer Form erfolgen.

Gegen die Veröffentlichung von Denkmallisten im Internet bestehen seit In-Kraft-Treten des IFG NRW keine durchgreifenden datenschutzrechtlichen Bedenken mehr.

6.6 Veröffentlichung von Bodenbelastungsdaten in Karten

Parzellenscharfe Informationen zur Lage von altlastverdächtigen Flächen, Altlasten und schädlichen Bodenveränderungen dürfen nur im Rahmen der Aufgabenerfüllung an die zuständigen Behörden übermittelt, aber nicht allgemein zugänglich gemacht werden.

Sollen solche Angaben veröffentlicht werden, bedarf es einer eigenen gesetzlichen Ermächtigung, soweit mit der Bekanntgabe von Daten an die Öffentlichkeit Eingriffe in das Recht auf informationelle Selbstbestimmung der Betroffenen verbunden sind. Nur wenn Angaben **sachbezogen** und nicht zugleich auf eine natürliche Person beziehbar sind, kann die Veröffentlichung - auch im Internet - als datenschutzrechtlich unproblematisch angesehen werden. Der **Personenbezug** lässt sich etwa herstellen, wenn aus dem Eintrag von Schadstoffen Aussagen über die Verursachereigenschaft abzuleiten sind. Erfolgt die Veröffentlichung von Daten über **altlastenverdächtige Flächen**, um die Öffentlichkeit über mögliche Gefahrenpunkte zu informieren, sind parzellengenaue Angaben über diese Flächen, etwa verbunden mit der Angabe über den Schadstoff, geeignet, schwerwiegende Nachteile für die Grundstückseigentümerinnen und -eigentümer zu bewirken; in ihr Recht auf informationelle Selbstbestimmung würde unverhältnismäßig eingegriffen. Ein solcher Eingriff wäre auch nicht von § 5 Abs. 2 Landes-Bodenschutzgesetz erlaubt, da nach dieser Norm die Verdachtsfälle nur in kommunalen Bodenbelastungskarten erfasst werden dürfen.

Zulässig ist eine Veröffentlichung, die **schadstoffbelastete Flächen ohne Personenbezug** darstellt. Dazu erscheint eine kartografische Darstellung im Maßstab 1:10000 oder 1:5000 (wenn sich die Angabe auf mehr als drei Privatgrundstücke bezieht) aus datenschutzrechtlicher Sicht hinnehmbar zu sein. Diese Bodenbelastungskarte kann ohne weiteres auch im Internet veröffentlicht werden.

7 Verkehr

7.1 TÜV Service Card - Service oder aufgedrängte Kundenbindung?

Der TÜV nutzte Daten, die im Rahmen der Kfz-Hauptuntersuchung erhoben werden, um seinen Kundinnen und Kunden eine Service Card mit verschiedenen Service- und Dienstleistungen anzubieten und sie damit an das Unternehmen zu binden. Einwilligungen der Betroffenen wurden nicht eingeholt.

In § 6 Abs. 2 Kraftfahrsachverständigengesetz ist ausdrücklich bestimmt, dass Sachverständige personenbezogene Daten, die ihnen bei ihrer Tätigkeit bekannt geworden sind, nur für diese Tätigkeit verwenden dürfen. Obwohl diese Daten der Kraftfahrzeughalterinnen und -halter mithin nur zu Dokumentationszwecken hätten gespeichert werden dürfen, wurden sie jedoch mit der Service Card - datenschutzwidrig - auch zum Zweck der Kundenbindung genutzt.

Die TÜV Service Card ist aus dem Verkehr gezogen worden.

7.2 Schüler-Schoko-Ticket mit bitterem Beigeschmack

Nordrhein-westfälische Verkehrsverbunde bieten das Schoko-Ticket, das nicht nur für die täglichen Schulfahrten, sondern auch in der Freizeit genutzt werden kann, allen Schülerinnen und Schülern im Jahresabonnement an. Allerdings forderten sie, in die Teilnahme am Lastschriftverfahren einzuwilligen und generell einer Bonitätsprüfung bei der Schufa zuzustimmen - ein Verstoß gegen den Datenschutz.

Die Verkehrsunternehmen führten die Bonitätsprüfung nicht vor jedem Vertragsschluss durch. Sie nutzten die Einwilligungserklärungen nur bei wiederholtem Auftreten von Rücklastschriften, um eine Schufa-Abfrage durchzuführen. **Generell** eine **Einwilligung** zur **Bonitätsprüfung** einzuholen ist unzulässig, da eine Bonitätsprüfung nur im Fall eines Zahlungsrückstandes erforderlich wird. In der Regel dient eine Bonitätsprüfung vor Vertragsschluss der Entscheidung, ob überhaupt ein Vertrag abgeschlossen werden soll. Diese Frage stellt sich beim Schoko-Ticket im Einzelfall meistens aber gar nicht. Ohne einen konkreten Anlass ist die Einholung dieser Einwilligung eine **unzulässige Datenerhebung auf Vorrat.**

Die Einwilligungserklärung zur Bonitätsprüfung bei Einzugsermächtigungen wurde aus den Antragsformularen gestrichen.

7.3 Elektronisches Fahrgeldmanagement

Bereits im 15. Datenschutzbericht 2001 unter 16.5, S. 138, wurde dargestellt, dass sich die Verkehrsverbunde Rhein-Ruhr (VRR) und Rhein-Sieg (VRS) mit der Möglichkeit des Einsatzes eines „elektronischen Fahrscheins" beschäftigen. Nunmehr soll ein einheitliches Verfahren möglichst bundesweit zum Einsatz kommen, bei dem elektronische Fahrscheine auf einer Chipkarte abgespeichert werden.

Aus diesem Grund haben mit dem Verband Deutscher Verkehrsunternehmen (VDV) Gespräche stattgefunden. In einer Arbeitsgruppe aus Vertreterinnen und Vertretern der Verkehrsunternehmen und der Aufsichtsbehörden für den Datenschutz wurden die datenschutzrechtlichen Auswirkungen des Verfahrens erörtert. Das Ergebnis ist ein Katalog, der die **datenschutzrechtlichen Grundanforderungen** an die Einführung eines elektronischen Fahrgeldmanagements bestimmt. Dieser Anforderungskatalog wurde mit der Datenschutzkonferenz und dem Düsseldorfer Kreis abgestimmt.

Die ausgearbeiteten Grundanforderungen behandeln im Wesentlichen die Bereiche **Transparenz**, **Datensparsamkeit** und **datenschutzgerechte Gestaltung der Systemkomponenten.**

Die Datenverarbeitung durch das elektronische Fahrgeldmanagement muss **transparent** im Sinne des § 6c Abs. 1 Nr. 2 und 3 BDSG sein. Dies erfordert die Festlegung der Zwecke und die Beschreibung der einzelnen Datenverarbeitungsvorgänge differenziert nach den jeweiligen für die Fahrgäste zutreffenden Geschäftsprozessen und der dabei zu verarbeitenden Daten. Notwendig sind Angaben der Identitäten und Anschriften der Stellen, die zu den genannten Zwecken personenbezogene Daten verarbeiten und/oder bei denen die jeweiligen Rechtsansprüche geltend gemacht und Verfahrensbeschreibungen gemäß § 4g Abs. 2 Satz 2 BDSG eingesehen werden können. Die Einbeziehung der Unterrichtungspflichten der Kundenvertragspartnerinnen und -partner ist unerlässlich. Dazu soll ein Merk- oder **Informationsblatt** erstellt werden, in dem die Fahrgäste in allgemein verständlicher Form über die vorgesehene Datenverarbeitung -

auch durch zentrale Servicestellen oder andere autorisierte Dritte - und über ihre Auskunfts- und Widerspruchsrechte unterrichtet werden.

Alle Leistungsmerkmale und Geschäftsprozesse sind nach dem Prinzip der **Datenvermeidung** und Datensparsamkeit (§ 3a BDSG) zu gestalten. Insbesondere dürfen keine Daten verarbeitet werden, die die Erstellung **kundenbezogener Bewegungsprofile** ermöglichen. Das bedeutet in erster Linie, Daten für Planungszwecke und zur Optimierung des Angebots bereits nur **anonym** zu erheben oder frühestmöglich zu anonymisieren. Soweit Daten für besondere Leistungsangebote oder das Reklamationsmanagement benötigt werden, sind diese **pseudonym** zu erheben und zu speichern, so dass ohne Wissen und Wollen der betroffenen Fahrgäste eine Zuordnung zu ihrer Person ausgeschlossen ist.

Die **Systemkomponenten**, die von Fahrgästen bedient werden, sind datenschutzgerecht so zu gestalten, dass keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten, zur Kenntnis zu nehmen. Fehlermeldungen der Zugangs-Erfassungssysteme dürfen die Betroffenen nicht öffentlich diskriminieren. Die Fahrgäste müssen in angemessenem Umfang die Möglichkeit haben, den Inhalt der Chipkarte jederzeit auslesen zu können.

Den Fahrgästen muss schließlich nach Information über die vertraglich bedingte Datenverarbeitung eine **freie Entscheidung** zwischen anonymer Fahrt und besonderen Leistungsangeboten (zum Beispiel best pricing) überlassen bleiben.

Auf der Grundlage dieses Anforderungskatalogs kann zukünftig bundesweit ein weitestgehend datenschutzgerechtes Management der elektronischen Fahrscheine sichergestellt werden.

7.4 Aufzeichnung von Telefongesprächen im Flughafenbetrieb

Piloten eines Luftfahrtunternehmens beschwerten sich, dass eine Flughafengesellschaft Telefongespräche ohne Kenntnis der Betroffenen aufzeichnete.

Es stellte sich heraus, dass die Aufzeichnung vorwiegend zur Beweissicherung für bestellte Dienste des Flughafenunternehmens und zur Abrechnung von Dienstleistungen der Flughafengesellschaft im Bodenver-

kehrsdienst erfolgte. Es handelte sich aber nicht um eine Vorkehrung zur Aufzeichnung von telefonischen Bombendrohungen. Eine Ermächtigungsgrundlage für die Aufzeichnung der Telefongespräche gab es nicht. Das Ministerium für Wirtschaft und Mittelstand, Energie und Verkehr NRW bestätigte, dass aus luftverkehrsrechtlicher Sicht **keine Notwendigkeit** zur Aufzeichnung von Telefongesprächen der Bodenverkehrsdienste bestünde. Zugelassen sind ausschließlich Aufzeichnungen von Funk- und Telefongesprächen durch die Luftaufsicht und durch die Flugsicherung.

Die Flughafengesellschaft wurde darauf hingewiesen, dass das Aufzeichnen dieser Gespräche unzulässig ist. Die Gesellschaft hat daraufhin die Aufzeichnung eingestellt.

7.5 Scannen von Passdaten beim Check-In

Viele Fluggäste mit dem Reiseziel USA wundern sich darüber, dass verschiedene Luftfahrtunternehmen beim Einchecken ihre Daten aus den Reisepässen einscannen.

Die Fluggesellschaften berufen sich auf amerikanische Einreisebestimmungen, wonach sie verpflichtet seien, nicht nur vor dem Flug die Voraussetzungen für eine Einreise zu prüfen, sondern auch bestimmte Daten noch während des Fluges an die amerikanischen Einwanderungsbehörden zu übermitteln. Dies verlange inzwischen auch Kanada. Den Fluggesellschaften würden für den Fall der „Nicht-Übermittlung" seitens der USA und Kanada empfindliche Sanktionen bis hin zum Landeverbot angedroht.

Diese **Datenerfassung aus Pässen** ist nach § 18 Abs. 3 Passgesetz **verboten**. Hiernach dürfen Passdaten von privaten Unternehmen weder zum automatischen Abruf noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Da dieses Verbot nur durch Änderung des Passgesetzes zu überwinden ist, wurde das Bundesministerium für Verkehr unterrichtet.

Fraglich ist, ob die zusätzlichen von den Einwanderungsbehörden gewünschten Daten - etwa Reservierungs- und Ticketdaten - zur Verfügung gestellt werden dürfen. Eine bereichsspezifische Rechtsgrundlage besteht für diesen Datentransfer nicht. Somit können die Daten nur aufgrund einer Einwilligung oder einer Abrede im Beförderungsvertrag in der vorgesehenen Weise verarbeitet werden. Eine Einwilligung der Fluggäste in

die Datenübermittlung scheidet als Rechtsgrundlage aus, da es an der erforderlichen Freiwilligkeit der Entscheidung fehlt: Die Verweigerung einer solchen „Einwilligung" würde nämlich unweigerlich zur Nicht-Beförderung führen. Deshalb wird erwogen, eine entsprechende Datenübermittlungsklausel in den **Beförderungsvertrag** mit aufzunehmen. Dabei ist aber auch zu prüfen, ob alle derzeit erhobenen Reservierungsdaten zur Erfüllung des Beförderungsvertrages benötigt werden.

Auf jeden Fall müssen die Fluggesellschaften ihren Fluggästen die Datenübermittlung an die Einwanderungsbehörden unverzüglich transparent machen.

7.6 „Miles & More" - Kundenbindungsprogramm einer Fluggesellschaft

„Wer hat Ihren Ferien-Flug bezahlt, Herr Minister?" - Diese Schlagzeile einer großen deutschen Boulevard-Zeitung bildete den Auftakt zu einem Vorgang, der als „Bonusmeilen-Affäre" in Erinnerung bleiben wird.

Eine Fluggesellschaft bietet im Rahmen ihres Kundenbindungsprogramms „Miles & More" unter anderem auch allen Bundestagsabgeordneten ihre „Senatoren-Karte" an, die es den Inhaberinnen und Inhabern ermöglicht, bei ihren Flügen mit dieser Fluglinie und bei der Inanspruchnahme von Dienstleistungen bestimmter Partnerunternehmen „Bonus-Punkte" zu sammeln, die sie gegen Prämien eintauschen oder zwecks bestimmter Vergünstigungen einsetzen können. Die Zeitung warf nunmehr in immer neuen Veröffentlichungen verschiedenen namentlich genannten Bundestagsabgeordneten gezielt vor, ihre bei Dienstflügen erworbenen Bonusmeilen zu privaten Zwecken eingesetzt zu haben, wobei dem Blatt offensichtlich **personenbezogene Daten** von Kundinnen und Kunden der Fluggesellschaft vorlagen.

In diesem Zusammenhang interessierte nicht die mit der „Affäre" einhergehende Diskussion um die Nutzungsmöglichkeiten der Senatorenkarte. Dagegen stellten sich generell Fragen nach **Datenschutz** und **Datensicherheit** im Rahmen des Kundenbindungsprogramms. Wie konnten Daten von Kundinnen und Kunden an die Öffentlichkeit gelangen? Welche personenbezogenen Daten werden wie und wo verarbeitet? Wie werden die Kundinnen und Kunden über diese Datenverarbeitung

aufgeklärt, und haben sie wirksam eingewilligt? Wer hat Zugriff auf die Daten? Sind ausreichende organisatorische und technische Sicherheitsmaßnahmen seitens der Verantwortlichen getroffen? Wie sich herausstellte, war aus dem Kreis der Beschäftigten eines Call-Centers eine Liste mit personenbezogenen Daten gezielt an Dritte weitergegeben worden. Ein solcher vorsätzlicher und von krimineller Energie getragener Datenschutzverstoß lässt sich bedauerlicherweise auch bei der Anwendung größtmöglicher Sorgfalt letztlich nie sicher vermeiden.

Ob und inwieweit das Kundenbindungsprogramm im Übrigen den Anforderungen des Datenschutzes und der Datensicherheit genügt, wird noch geprüft. Die Fluggesellschaft ist selbst an einer datenschutzgerechten und datensicheren Konzeption und Umsetzung interessiert.

8 Handel, Auskunfteien und Kreditwirtschaft

8.1 Verwendung von Personalausweisen bei Banken, im Handel und für Selbstauskünfte bei Auskunfteien

Vermehrt fragen Bürgerinnen und Bürger nach der Rechtmäßigkeit des Vorgehens, wenn sie im nicht-öffentlichen Bereich gebeten werden, sich entweder mit einem Personalausweisdokument auszuweisen oder Daten aus ihrem Personalausweis notieren oder speichern zu lassen.

Es geht beispielsweise um folgende Fallkonstellationen: Bei der **Eröffnung eines Kontos** sind **Kreditinstitute** nach der Abgabenordnung gehalten, sich Gewissheit über Person und Anschrift der Verfügungsberechtigten zu verschaffen und sicherzustellen, dass sie jederzeit darüber Auskunft geben können, über welche Konten eine Person verfügungsberechtigt ist. In der Praxis verschaffen sich Kreditinstitute diese Gewissheit, indem sie den vollständigen Namen und die Anschrift anhand eines gültigen Personalausweises oder Reisepasses feststellen. Dazu notieren sie Geburtsdatum, Anschrift sowie Art, Nummer und ausstellende Behörde des Personalausweises oder Reisepasses auf dem Kontoeröffnungsantrag, der in der Kontoakte abgelegt wird.

Diese Verfahrensweise war deshalb zweifelhaft, weil die Kreditinstitute entsprechend den Verlautbarungen des Bundesaufsichtsamtes für das Kreditwesen bei Kontoeröffnungen die Identifizierung gemäß dem Geldwäschegesetz (GwG) (siehe hierzu unter 8.5.2) vornahmen, ohne dass jedoch dessen Voraussetzungen hierfür erfüllt waren. Die Identifizierung war aber dann datenschutzrechtlich nicht zu beanstanden, wenn die Notierung der Personalausweisdaten im Einvernehmen mit der Kundin oder dem Kunden auch auf die vorweggenommene Erfüllung der Anforderungen nach dem GwG gestützt wurde. Inzwischen hat sich diese Problematik jedoch mit dem In-Kraft-Treten des Gesetzes zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus am 15. August 2002 erledigt. Neben zahlreichen anderen Änderungen wurde die **Identifizierungspflicht** auf Vertragsabschlüsse zur Begründung einer auf Dauer angelegten Geschäftsbeziehung ausgedehnt, wozu insbesondere die Führung eines Kontos zählt. Damit hat die Praxis der Kreditinstitute bei Kontoeröffnungen eine eindeutige gesetzliche Legitimation gefunden.

Wenn eine Kundin oder ein Kunde im **Handels- und Dienstleistungsbereich** bargeldlos mit der EC-Karte bezahlen möchte, wird

immer häufiger die Vorlage des Personalausweises verlangt, was oftmals zu Irritationen bei den Betroffenen führt, weil sie davon ausgehen, nur Behörden seien dazu berechtigt. Grundsätzlich ist hierzu zu sagen, dass § 4 Abs. 1 des Gesetzes über Personalausweise (PAuswG) die Vorlage von Personalausweisdokumenten auch im nicht-öffentlichen Bereich erlaubt. Danach können der **Personalausweis** und der vorläufige Personalausweis auch im nicht-öffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden. Das PAuswG verbietet lediglich, die Seriennummern der Ausweise so zu verwenden, dass mit ihner ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Außerdem darf der Personalausweis weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung solcher Daten verwendet werden.

Wird bei einem **Umtausch von Ware** neben dem Namen und der Anschrift der Kundin oder des Kunden auch die Nummer des Personalausweises auf der Rückseite des Kassenbons notiert, ist dies unzulässig. Die Unternehmen begründeten ihre Vorgehensweise damit, dass sie etwaigen Manipulationen durch das Personal vorbeugen oder diese aufdecken wollten. Soweit hierfür Name und Anschrift erhoben werden, ist dies datenschutzrechtlich noch tolerabel, weil die Unternehmen damit eigene berechtigte Interessen im Sinne des § 28 Abs. 1 Nr. 2 BDSG wahrnehmen. Nicht erforderlich und deshalb **unzulässig** ist es dagegen, darüber hinaus die **Personalausweisnummer** zu notieren (siehe hierzu unter 8.3.2).

Auskunfteien wie beispielsweise die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) sind gesetzlich verpflichtet, Betroffenen eine Selbstauskunft zu erteilen, damit diese erfahren können, welche Daten zu ihrer Person dort gespeichert sind. Häufig wird in diesem Zusammenhang angefragt, ob Auskunfteien berechtigt sind, vorab eine Kopie des Personalausweises anzufordern, wenn schriftlich eine Selbstauskunft beantragt wird. Die Auskunfteien weisen darauf hin, dass die Ausweiskopie ausschließlich der Identitätsüberprüfung dient. Damit solle der relativ hohen Zahl missbräuchlicher Abrufe von „Selbst"-Auskünften durch **Nichtberechtigte** begegnet werden. Die Ausweiskopien würden im Anschluss an die Identitätsprüfung fachgerecht vernichtet. Eine **eindeutige Identifizierung** der um Auskunft ersuchenden Person ist zulässig und sogar geboten. Dafür die Vorlage des Personalausweises oder einer entsprechenden Kopie zu verlangen, ist gemäß § 4 Abs. 1 PAuswG grundsätzlich erlaubt. Für die Identifizierung benötigten die Auskunfteien auf der Ausweiskopie indes

nur Name, Anschrift und Geburtsdatum. Alle **anderen** auf der Kopie befindlichen **Daten** können daher von den betroffenen Personen **geschwärzt** werden.

Falls Betroffene die Übersendung einer Ausweiskopie ablehnen, können sie bei der Auskunftei auch persönlich vorsprechen und den Ausweis lediglich vorlegen. Diese Form der Selbstauskunft hat gegenüber der schriftlichen auch den Vorteil der Unentgeltlichkeit.

8.2 Verbraucherschutz durch Information

Verbraucherinformationen werden als notwendige Grundlage für ein selbstbewusstes und eigenverantwortliches Konsumverhalten anerkannt. Immer häufiger wird dabei die Frage gestellt, ob Warnhinweise öffentlich bekannt gegeben werden dürfen.

Eine **Lebensmittelüberwachungsbehörde** will darüber aufklären, dass die Wurst eines Herstellers auch - was sich aus der Zutatenauflistung nicht ergibt - Rindfleisch enthält. Dies ist zu Zeiten von BSE für viele Verbraucherinnen und Verbraucher eine wichtige Information. Diese Information muss aber auch die Herstellerin oder den Hersteller bezeichnen. Ob dies bei **natürlichen Personen** datenschutzrechtlich zulässig ist, wird durch spezialgesetzliche Vorschriften - wie das Lebensmittel- und Bedarfsgegenstände-Vollzugsgesetz NRW - nicht geklärt, da diese Gesetze selbst keine Veröffentlichungsbefugnis vorsehen. Nach dem DSG NRW wäre eine Veröffentlichung nur zulässig, wenn die Herstellerfirma nicht widersprochen hat.

In anderen Fällen kommt es darauf an, ob eine **Preisgabe** personenbezogener Daten **erforderlich** ist. Ist es zur Aufklärung der Verbraucherinnen und Verbraucher auch erforderlich, dass das zuständige **Veterinäramt** öffentlich den landwirtschaftlichen Betrieb bezeichnet, in dem ein BSE-Verdacht festgestellt wurde? Die gleiche Frage stellt sich bei Schweinepest und Maul- und Klauenseuche. Natürlich lässt es sich nicht vermeiden, dass die seuchenrechtlich vorgeschriebenen Maßnahmen - wie Absperrungen und das Entfernen getöteter Tiere - der Öffentlichkeit bekannt werden. Es macht aber keinen Sinn, wenn die zuständige Behörde den Betrieb und mit ihm auch die betroffene Landwirtin oder den Landwirt zu allem Unglück durch Veröffentlichungen auch noch an den Pranger stellen. Die Behörde hat dafür zu sorgen, dass die notwendigen Abwehrmaßnahmen ergriffen werden; die Verbraucherinnen und Verbraucher können selbst keine weitere Vorsorge zu

ihrem eigenen Schutz treffen. Deshalb ist die Preisgabe personenbezogener Daten hier nicht erforderlich und damit **unzulässig**.

Anders sind dagegen - auch vom Bundesverfassungsgericht für zulässig erachtete - **Warnhinweise** über belastete oder verdorbene **Lebensmittel** zu beurteilen, die bereits in den Verkehr gebracht worden sind. Hier besteht die behördliche Pflicht, weitere Schäden durch Verzehr zu vermeiden, auch wenn dabei die Herstellerfirma und das Produkt benannt werden müssen. Besser wäre allerdings, in einem Verbraucherinformationsgesetz die Befugnisse der zuständigen Überwachungsbehörden zur Veröffentlichung auch personenbezogener Daten normenklar zu regeln.

Eingriffe in das Persönlichkeitsrecht können auch von privaten Verbänden oder Vereinen vorgenommen werden. Es gab im Berichtszeitraum Fälle, die von den Betroffenen als Anprangerung verstanden wurden, sich bei gründlicher Prüfung aber als zulässige Aufklärung herausstellten. Dies war zum Beispiel bei einer auf der **Website einer Umweltorganisation** veröffentlichten Übersicht der Fall, in der mit Angaben aus öffentlich zugänglichen Unterlagen die Tätigkeiten von Funktionären landwirtschaftlicher Organisationen in Aufsichtsräten oder als Gesellschafter landwirtschaftlicher Unternehmen dargestellt wurden.

In einem anderen Fall veröffentlichte eine große **Verbraucherorganisation** Hinweise von Verbraucherinnen oder Verbrauchern über Preiserhöhungen im Zusammenhang mit der **Euro-Einführung** auf ihrer Website. Da in der Übersicht auch Einzelhandelsfirmen, Gaststätten und andere Betriebe genannt wurden, hinter denen natürliche Personen als Inhaberinnen und Inhaber stehen, wirft diese Veröffentlichung auch eine datenschutzrechtliche Problematik auf. Teilweise wird eine solche Veröffentlichung als bedenkliche Anprangerung verstanden. Im Wesentlichen enthalten die veröffentlichten Daten - allgemein zugängliche - Preisangaben über bestimmte Produkte in DM und Euro sowie die Stellungnahmen der gleichfalls benannten Firmen und Betriebe. Nach Prüfung der Hinweise auf Plausibilität werden die Firmen oder Betriebe angeschrieben, über die Absicht der Verbraucherorganisation aufgeklärt und um Stellungnahme zu den Gründen für die Preiserhöhung gebeten. In gegebenenfalls notwendigen Erinnerungsschreiben wird noch einmal um eine Stellungnahme gebeten, zugleich aber darauf hingewiesen, dass Preis- und Produktangaben auch ohne eine solche Stellungnahme veröffentlicht würden. Der Bitte von Unternehmen, den sie betreffenden Hinweis nicht zu veröffentlichen, kommt die Verbraucherorganisation allerdings nach. Den Interessen der

Verbraucherinnen und Verbraucher sowie der Allgemeinheit, die Hintergründe von Preiserhöhungen im Zuge der Euro-Einführung zu erfahren, stehen im Hinblick auf diese Verfahrensweise **keine schutzwürdigen Interessen** der betroffenen Firmen und Betriebe entgegen.

Aus diesen Gründen wurde lediglich empfohlen, aus der Übersicht die Namen der Inhaberinnen und Inhaber zu löschen. Gegen die Bezeichnung des Unternehmens bestehen keine Bedenken.

8.3 Handel

8.3.1 Abwehr unerwünschter Werbezuschriften

In den Top Ten der Anfragen zum Datenschutz in der Wirtschaft kamen Beschwerden über unerwünschte Werbung und Adresshandel in den letzten beiden Jahren stets auf einen der vorderen Plätze. Die zahlreichen Beschwerden zeigen: Unerwünschte Werbung regt viele Bürgerinnen und Bürger mehr auf als an. Sie fühlen sich belästigt und bitten um Hinweise, wie sie die Flut unerwünschter Werbung eindämmen und von ihren Briefkästen, Faxen, Telefonen und PC fernhalten können.

Um auf diese große Nachfrage reagieren zu können, wurde in Zusammenarbeit mit einigen norddeutschen Landesbeauftragten das Faltblatt „Bitte keine Werbung - Tipps und Informationen zu Adresshandel und unerwünschter Werbung" herausgegeben. Vielen Beschwerden liegt der weit verbreitete Irrtum zugrunde, dass Unternehmen die Namen und Adressen ihrer Kundinnen und Kunden stets nur mit deren Einwilligung für Werbezwecke weitergeben und nutzen dürfen. Tatsächlich ist der Bundesgesetzgeber diesem aus Sicht des Daten- und Verbraucherschutzes wünschenswerten Anliegen aber nicht nachgekommen. Auch nach dem novellierten BDSG ist daher die Übermittlung und Nutzung von Adressen für Werbezwecke grundsätzlich zulässig - ohne dass es auf eine Einwilligung der Betroffenen ankäme.

Nach § 28 Abs. 3 Nr. 3 BDSG dürfen bestimmte personenbezogene Daten - insbesondere Name, Anschrift und Geburtsjahr - für Zwecke der Werbung genutzt und übermittelt werden, solange die Betroffenen **nicht widersprechen** oder die verantwortliche Stelle nicht aus sonstigen Gründen annehmen muss, dass ein schutzwürdiges Interesse am Ausschluss der Übermittlung und Nutzung besteht.

Anders ist es dagegen bei der Übermittlung und Nutzung sonstiger personenbezogener Daten - zum Beispiel zum Kauf- oder Zahlungsverhalten - und bei der Nutzung von Tele- und Mediendiensten im Internet, beispielsweise beim Electronic Banking oder bei Warenbestellungen im Internet. Hier ist eine Weitergabe der Daten zu Werbezwecken stets nur mit **ausdrücklicher Einwilligung** der jeweiligen Person zulässig.

Ansonsten gilt: Erst wenn die Betroffenen gegenüber der verantwortlichen Stelle (etwa der werbenden Firma oder dem Adresshändler) ihr **Widerspruchsrecht** geltend machen, werden Adressenhandel und Werbung unzulässig. Dazu müssen sie erklären, dass ihre Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung weder genutzt noch weitergegeben werden sollen.

Die Betroffenen können den **Widerspruch jederzeit einlegen**, also auch bereits dann, wenn sie ihre persönlichen Daten erstmals gegenüber dem Geschäfts- oder Vertragspartner angeben. Damit können sie erreichen, dass es gar nicht erst zur Zusendung erster Werbebriefe kommt.

Häufig verlangen Bürgerinnen und Bürger neben dem Widerspruch auch die **Löschung** ihrer Adressdaten. Dennoch können sie Werbung erhalten, wenn das Unternehmen später Adressen kauft oder anmietet und ihre Daten wieder in diesen Adressbeständen enthalten sind. Sinnvoller als das Löschen ist es daher, es hinsichtlich der Adressdaten bei dem Widerspruch zu belassen. Die Adresse muss dann in eine **Werbe-Sperrdatei** aufgenommen werden. Das ermöglicht die Prüfung, ob zu den jeweils neu erworbenen Anschriften bereits ein Widerspruch vorliegt.

Um herauszufinden, von wem das werbende Unternehmen oder der Adresshändler die Daten erhalten und an wen sie weitergegeben wurden, können die Betroffenen ihr **Auskunftsrecht** gegenüber der speichernden Stelle geltend machen (§ 34 Abs. 1 BDSG). Danach kann jede Person beispielsweise von dem werbenden Unternehmen oder dem Adresshändler Auskunft verlangen über die zur eigenen Person gespeicherten Daten, ihre Herkunft, den Zweck der Speicherung und die Empfänger oder die Kategorien von Empfängern, an die gegebenenfalls Daten weitergegeben werden. Nur wenn ein Adresshändler begründet darlegt, dass er ein überwiegendes Geschäftsgeheimnis zu wahren hat, kann er die Auskunft zu Herkunft und Empfänger der Daten verweigern. Damit das jeweilige Unternehmen die Herkunft der Adresse ermitteln kann, ist es im Übrigen

hilfreich, diesem die oftmals auf der Werbesendung enthaltene **Code-Nummer** mitzuteilen.

Schließlich helfen den Betroffenen die beiden im Zuge der Novellierung des BDSG neu geschaffenen **Unterrichtungspflichten** nach §§ 4 Abs. 3 und 28 Abs. 4: Hat ein Unternehmen, ein Verein oder eine sonstige Organisation vor, die Kunden- oder Mitgliederdaten nicht nur für den vereinbarten Zweck, sondern beispielsweise auch für Werbezwecke zu verarbeiten oder zu nutzen, so müssen die betroffenen Personen bereits bei Erhebung ihrer Daten über diese Zwecke und die möglichen Arten von Empfängerinnen und Empfängern der Daten **unterrichtet** werden (§ 4 Abs. 3 BDSG). Darüber hinaus hat die verantwortliche Stelle, also etwa das werbende Unternehmen, die Adressatinnen und Adressaten spätestens mit dem Werbeschreiben über das Widerspruchsrecht und die Identität der verantwortlichen Stelle zu informieren. Wenn der Absender Daten nutzt, die bei einer ihm nicht bekannten Stelle gespeichert werden - weil er beispielsweise ein Unternehmen mit der Werbung beauftragt hat, das wiederum eine Adresshandelsfirma eingeschaltet hat -, muss er auch sicherstellen, dass die betroffenen Personen **Kenntnis über die Herkunft** der Daten erhalten können (§ 28 Abs. 4 Satz 2 BDSG). Unternehmen, die gezielt durch Verlosungen, Preisausschreiben, Haushaltsbefragungen oder bei Informationsveranstaltungen Daten erheben, um sie anschließend für Werbezwecke zu verwenden oder zu veräußern, müssen bereits bei der **Datenerhebung** über diesen Zweck, über die Empfängerinnnen und Empfänger, über das Widerspruchsrecht und über die verantwortliche Stelle **informieren**.

Weitere Hinweise und Hilfestellungen zu dem Thema, insbesondere auch zu unerwünschter Fax-, SMS- und E-Mail-Werbung, enthält das Faltblatt "Bitte keine Werbung - Tipps und Informationen zu Adresshandel und unerwünschter Werbung ", das angefordert werden kann. Der Text ist auch unter www.lfd.nrw.de abrufbar. Für werbegeplagte Bürgerinnen und Bürger hat es sich im Übrigen als sehr hilfreich erwiesen, Fragen, Beschwerden und Auskunftsbegehren direkt an die betrieblichen Datenschutzbeauftragten der jeweiligen Unternehmen zu richten. Diese kennen das Datenschutzrecht meistens besser als die Marketingabteilung und haben daher in der Regel auch ein größeres Verständnis für die entsprechenden Anliegen.

8.3.2 Bezahlung mit EC-Karte

Im Handels- und Dienstleistungsbereich ist es heute fast überall möglich und gängig, im Wege des bargeldlosen Zahlungsverkehrs einzukaufen. Dabei führt es immer wieder zu Irritationen bei Bürgerinnen und Bürgern, dass Händler zunehmend die Personalausweisdaten der Kunden notieren oder laut Lastschriftbeleg Daten an Dritte übermitteln.

Bargeldlose Zahlungen werden bei Handels- und Dienstleistungsunternehmen häufig durch Vorlage der EC-Karte abgewickelt. Vielfach wird im Handel das **elektronische Lastschriftverfahren (ELV)** eingesetzt, bei dem die Kundinnen und Kunden eine Abbuchungsermächtigung über den Rechnungsbetrag erteilen. Dabei dient die EC-Karte lediglich zum Auslesen der Bankverbindung und als Nachweis für die Existenz eines Girokontos. Die EC-Funktionalität der Karte wird nicht genutzt.

Der technische Verfahrensablauf sieht - verkürzt dargestellt - wie folgt aus: Wird die EC-Karte zur Bezahlung vorgelegt, werden die Kontonummer und die Bankleitzahl (Bankverbindung) aus der EC-Karte ausgelesen. Über das Terminal im Geschäft wird die Bankverbindung mit einer Sperrdatei und einer Datei über Zahlungslimits abgeglichen. Sind die Daten der Betroffenen nicht in den Dateien enthalten, wird der Zahlungsvorgang mit „O.K." bestätigt und zusammen mit den Daten über den Kauf im Terminal des Geschäfts in einem so genannten Transaktionsdatensatz gespeichert. Mit dem „O.K." wird eine Lastschrifteinzugsermächtigung ausgedruckt. Auf dieser befindet sich auch der Text einer Erklärung, mit der die Kundinnen und Kunden in die Bekanntgabe der Anschrift von Kontoinhaberin oder Kontoinhaber durch die Bank an das Geschäft im Falle einer Rücklastschrift einwilligen. Die unterschriebenen Belege verbleiben im Geschäft. Die so tagsüber angesammelten Transaktionsdatensätze werden in der Regel einmal pro Nacht auf elektronischem Wege bei den Banken zur Lastschrift eingereicht und dann dem Konto des Geschäfts gutgeschrieben.

Nach diesem Verfahren wird die Ware also nicht gleich von der Bank bezahlt. Vielmehr gewährt das Unternehmen beim Bezahlen mittels ELV einen Warenkredit ohne Sicherheiten bis zur Einlösung der Lastschrift. Der Einkauf ist nämlich erst „bezahlt", wenn die Lastschrift auf dem Konto des Unternehmens gutgeschrieben ist.

Der auf dem Lastschriftbeleg enthaltene **Hinweis**, dass die Angaben über die Bankverbindung an andere Unternehmen übermittelt werden, bedeutet lediglich, dass im Falle der Nichteinlösung der Lastschrift die Angaben über die Bankverbindung an andere Unternehmen übermittelt werden dürfen, die ebenfalls dieses Lastschriftverfahren anwenden. Die Speicherung und die Übermittlung sind nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG beziehungsweise bei einer gemeinsamen Sperrdatei der am Abrechnungssystem angeschlossenen Unternehmen nach § 29 Abs. 1 und Abs. 2 BDSG zulässig. Hierzu bedarf es nicht der Einwilligung der Kundin oder des Kunden. Eine Nutzung der Daten zu Werbezwecken ist nicht erlaubt.

Auch die bei einigen Unternehmen ab einem bestimmten Warenwert übliche Erhebung von Name und Anschrift der Kundinnen und Kunden ist nicht zu beanstanden und gemäß § 28 Abs. 1 Nr. 1 BDSG zulässig. Der Grund für diese Datenerhebung liegt darin, dass die Bank zwar durch die auf dem Beleg unterschriebene Einzugsermächtigung befugt ist, im Falle der Nichteinlösung Name und Anschrift bekannt zu geben. Eine Verpflichtung hierzu besteht jedoch nicht, teilweise werden diese Auskünfte auch von den Banken abgelehnt. Die Erhebung und Speicherung dieser Daten dient daher dem Interesse des Handelsunternehmens, sich vor Forderungsausfällen zu schützen und ist im Rahmen der Zweckbestimmung des Kauf- und Warenkreditvertrags von § 28 Abs. 1 Nr. 1 BDSG gedeckt. Dabei ist die Vorlage des **Personalausweises**, aus dem Name und Anschrift entnommen werden, ebenfalls nicht zu beanstanden. Nach § 4 Abs. 1 Personalausweisgesetz darf der Personalausweis auch im nicht-öffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden (siehe hierzu unter 8.1). Das Notieren der Personalausweisnummer und das Kopieren des Ausweises ist jedoch anders zu beurteilen. Dieses Vorgehen ist tatsächlich nicht erforderlich und damit datenschutzrechtlich unzulässig.

Kundinnen und Kunden, die mit der Erhebung und Speicherung ihrer Adressdaten nicht einverstanden sind, können anonym bleiben, indem sie bar bezahlen.

8.3.3 Kundenbindungsprogramme - weit mehr als ein elektronisches Rabattsystem

Viele können sich vielleicht noch an Zeiten erinnern, in denen sie bei ihren Einkäufen vor allem im Lebensmittelladen um die Ecke fleißig Rabattmarken sammelten, um sie in ein entsprechendes Heftchen

einzukleben und später einzulösen. Für die Jüngeren erscheint dies im Zeitalter der Plastikkarten wie eine Mär aus alten Zeiten.

Kundenkarten, mit denen Punkte gesammelt werden, die anschließend in Form von Prämien eingelöst werden oder die Preisnachlässe gewähren, sind „in". Die Unternehmen sind aus Gründen der **Kundenbindung** und des Marketings sehr daran interessiert. Für die Verbraucherin und den Verbraucher liegt der Vorteil auf der Hand: Er oder sie spart Geld. Allerdings gerät dabei oft in Vergessenheit, dass nun - mit dem Einsatz der Kundenkarte - selbst bei einem **Barkauf**, der bei vielen Geschäften des täglichen Lebens völlig anonym abgewickelt wird, unausweichlich **Datenspuren** hinterlassen werden, die es ermöglichen, Profile über das Kaufverhalten zu erstellen. Kundenbindungsprogramme bergen daher das Risiko „gläserner" Kundinnen und Kunden. Es ist also ein durchaus kritischer Umgang mit Kundenkarten angebracht und die weitere Entwicklung in diesem Bereich aufmerksam zu beobachten. Soweit die datenschutzrechtlichen Vorgaben eingehalten werden, können gegen diese Art von Rabattsystemen allerdings keine durchgreifenden Bedenken geltend gemacht werden.

Im Berichtszeitraum suchten zwei nordrhein-westfälische Unternehmen um Beratung zu einer unternehmensübergreifenden Kundenkarte nach, die für weitere Partnerunternehmen offen ist. Wie in vergleichbaren Konstellationen auch wurde eine rechtlich selbständige Betreibergesellschaft gegründet, die das **Bonusprogramm** für die beteiligten Unternehmen abwickelt.

Die Teilnahme an einem solchen Bonusprogramm richtet sich datenschutzrechtlich zunächst nach § 28 Abs. 1 Nr. 1 BDSG. Denn es kommt ein Vertrag zustande, der die Unternehmen aufgrund der jeweiligen Teilnahmebedingungen verpflichtet, Prämien oder Geld für gesammelte Punkte zu gewähren. § 28 Abs. 1 Nr. 1 BDSG erlaubt das Erheben, Speichern oder Übermitteln personenbezogener Daten als Mittel zur Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit der betroffenen Person dient. Die zur Programmabwicklung erforderliche Verarbeitung personenbezogener Daten, wie Name, Anschrift, Zahl der gesammelten Punkte, Art der gekauften Waren (hier reicht allerdings die Angabe der Warengruppe aus) ist also zulässig. Eine **Übermittlung** dieser Daten an Partnerunternehmen, bei denen keine Punkte gesammelt wurden, ist dagegen für den Vertragszweck nicht erforderlich und daher **grundsätzlich unzulässig**.

Sollen die personenbezogenen Daten auch für Werbe- und Marktforschungszwecke genutzt und verarbeitet werden, bedarf es dafür einer **ausdrücklichen Einwilligung** der am Kundenbindungsprogramm beteiligten Personen. Die bloße Gewährung einer Widerspruchsmöglichkeit reicht nicht aus. Um eine **wirksame Einwilligung** erteilen zu können, müssen die Betroffenen vorher darüber informiert sein, welche Daten zu welchem Zweck und von wem verarbeitet werden sollen. Dies muss aus der Einwilligungserklärung deutlich hervorgehen. Sie muss die üblichen Transparenzanforderungen erfüllen, die auch die Rechtsprechung verlangt und damit unter anderem auch separat platziert und gesondert unterschrieben oder angekreuzt werden.

Es bleibt zu hoffen, dass möglichst viele Unternehmen ihre Bonusprogramme künftig datenschutzkonform gestalten. Nur mit einer datenschutzrechtlich einwandfreien Einwilligungserklärung dürfen die umfassend gesammelten personenbezogenen Daten der teilnehmenden Kundinnen und Kunden für Werbe- und Marktforschungszwecke genutzt und verarbeitet werden. Eine entsprechende Einwilligung kann von vornherein verweigert, aber auch später noch widerrufen werden, ohne dass dies Auswirkungen auf die Teilnahme am Rabattprogramm hat.

8.3.4 Zusatzfunktion auf dem Geldkartenchip für den Jugendschutz

Ein eher ungewöhnliches Vorhaben plant der Bundesverband Deutscher Tabakwaren-Großhändler und Automatenaufsteller e.V. (BDTA):

Im Zuge des im Sommer 2002 novellierten Jugendschutzgesetzes wurden die Vorschriften zum Tabakkauf für Kinder und Jugendliche unter 16 Jahren verschärft. So ist die gewerbliche Abgabe von Tabak an diesen Personenkreis verboten. Tabakwaren dürfen in der Öffentlichkeit nicht in Automaten angeboten werden, es sei denn, es ist durch technische Vorrichtungen sichergestellt, dass Kinder und Jugendliche unter 16 Jahren Tabakwaren nicht entnehmen können. Für die technische Umrüstung gilt eine Frist bis zum 01. Januar 2007.

Im Laufe des Gesetzgebungsverfahrens hatte der BDTA verschiedene technische Möglichkeiten zur Umsetzung der Regelung für Zigarettenautomaten prüfen lassen und war zu dem Schluss gekommen, dass wegen des hohen Verbreitungsgrades der EC-Karte eine **Zusatzfunktion** auf dem dortigen **Geldkartenchip** eine geeignete technische Lösung darstelle.

Zu diesem Zweck sollte auf der EC-Karte in einem von der Geldkartenfunktion abgeschotteten Bereich das verschlüsselte **Geburtsdatum** der Karteninhaberinnen und -inhaber gespeichert werden. Die Zigarettenautomaten sollten technisch so umgerüstet werden, dass ein Modul in der Lage ist, nach Einführung der EC-Karte in den Automaten das Geburtsdatum anonymisiert auszulesen und je nach dem Ergebnis - über oder unter 16 Jahre - den weiteren Verkaufsvorgang frei zu geben oder nicht. Zur Umsetzung dieser Idee war unter anderem auch eine Prüfung der damit verbundenen datenschutzrechtlichen Probleme erforderlich, die vom BDTA frühzeitig eingeleitet wurde und unter Federführung von Nordrhein-Westfalen für den Düsseldorfer Kreis erfolgte.

Unabhängig von der Frage, ob die vom BDTA favorisierte Lösung über die EC-Karte tatsächlich die sinnvollste Möglichkeit darstellte, ergaben sich vor allem wegen der beabsichtigten **Speicherung des Geburtsdatums** datenschutzrechtliche Zweifel. Der überwiegende Anteil der EC-Karteninhaberinnen und -inhaber ist volljährig und damit zweifellos berechtigt, Zigaretten am Automaten zu erwerben. Um den geringen Teil der unter 16jährigen (und damit zwangsläufig auch diejenigen, die eine solche Karte gar nicht besitzen) vom Automatenkauf auszuschließen, sollte also das Geburtsdatum einer **Vielzahl Nichtbetroffener** gespeichert werden. Dies war mit dem Grundsatz der Datenvermeidung und Datensparsamkeit des § 3a BDSG nicht in Einklang zu bringen. Außerdem wäre für die Aufbringung des Geburtsdatums eine Einwilligungserklärung erforderlich gewesen, deren Einholung bei etwa 50 Millionen EC-Karten auf außerordentliche praktische Schwierigkeiten gestoßen wäre.

Nach weiteren Verhandlungen mit dem BDTA und der Kreditwirtschaft konnte eine Lösung erreicht werden, die dem Anliegen des BDTA Rechnung trägt und gleichzeitig den datenschutzrechtlichen Anforderungen der Aufsichtsbehörden genügt. Diese Lösung sieht kurz skizziert folgendermaßen aus:

Die erwachsenen EC-Karteninhaberinnen und -inhaber erhalten auf der Zusatzfunktion des Geldkartenchips lediglich einen so genannten **Legitimationsvermerk**, dem der Automat entnimmt, dass die betreffende Person nicht vom Schutzbereich des Jugendschutzgesetzes erfasst und der nachfolgende Verkaufsvorgang somit erlaubt ist.

Bei **Minderjährigen** wird das verschlüsselte Datum gespeichert, an dem sie die Volljährigkeit erreichen („**Jugendschutzsperrvermerk**"). Der Automat

vergleicht dann dieses Datum mit dem aktuellen Datum, an dem er bedient wird, errechnet daraus, ob die Person das 16. Lebensjahr vollendet hat und bricht je nach dem Ergebnis den Kaufvorgang ab oder gibt ihn frei. Die Kreditinstitute werden bei Anträgen Minderjähriger auf Ausstellung einer kontogebundenen Bankkarte mit Geldkartenchip die **Einwilligung** zur Speicherung des Volljährigkeitsdatums einholen.

Enthält ein Geldkartenchip keinen dieser Vermerke, ist ein Zigarettenkauf am Automaten nicht möglich, da nicht ermittelt werden kann, ob das 16. Lebensjahr vollendet ist. Der Einsatz der EC-Karte zur **Legitimation** am Zigarettenautomaten bedeutet nicht, dass bei einem freigegebenen Kaufvorgang nur noch mit der Geldkartenfunktion bezahlt werden kann. Vielmehr kann weiterhin bar bezahlt werden.

Die technische Umsetzung des Konzeptes wird weiter unter Beteiligung des Düsseldorfer Kreises begleitet. Die bisherige Zusammenarbeit mit den beteiligten Verbänden lässt erwarten, dass für beide Seiten zufriedenstellende Ergebnisse erreicht werden können.

8.4 Auskunfteien

8.4.1 Auskunftsanspruch nach dem neuen Bundesdatenschutzgesetz

In Umsetzung der EG-Richtlinie 95/46 wurde § 34 BDSG geändert und der Auskunftsanspruch der Betroffenen gegenüber der Stelle, die Daten zu ihrer Person verarbeitet oder sonst nutzt, erweitert. Von der Änderung sind im Wesentlichen Unternehmen betroffen, die personenbezogene Daten zum Zwecke der Übermittlung speichern, also Auskunfteien.

Diese Erweiterung des Auskunftsrechts hat in etlichen Fällen zu **Meinungsverschiedenheiten** über die Reichweite der neuen gesetzlichen Regelung geführt. Auch die Arbeitsgruppe „Auskunfteien" des Düsseldorfer Kreises (in dem die Aufsichtsbehörden der Länder im nicht-öffentlichen Bereich vertreten sind) konnte trotz mehrfacher Erörterung der Thematik noch keine Einigung mit dem betreffenden Wirtschaftsverband erzielen.

Bereits nach der früheren Rechtslage musste den Betroffenen grundsätzlich Auskunft über die zu ihrer Person gespeicherten Daten und deren Herkunft, über Empfängerinnen und Empfänger sowie über den Zweck der

Speicherung erteilt werden. Die Pflicht, Datenherkunft und -empfänger zu benennen, galt jedoch bislang für Unternehmen, die Daten geschäftsmäßig speichern, um sie an Dritte zu übermitteln (zum Beispiel Auskunfteien) nur dann, wenn die Betroffenen begründete Zweifel an der Richtigkeit der Daten geltend machen konnten. Diese **Einschränkung** wurde durch die Änderung des § 34 BDSG **aufgehoben**. Nunmehr sind Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern, grundsätzlich verpflichtet, Herkunft und Empfänger zu benennen. Eine Auskunft über Herkunft und Empfänger kann jetzt nur noch verweigert werden, wenn dem ein überwiegendes Interesse an der Wahrung des Geschäftsgeheimnisses entgegensteht.

Unstrittig ist, dass bei **fehlerhaften Daten** auf keinen Fall eine Auskunft unter Berufung auf das Geschäftsgeheimnis verweigert werden kann. Gerade in diesen Fällen hat die betroffene Person ein überragendes Interesse an der Kenntnis von Herkunft und Empfänger, schon um dort die Berichtigung oder Löschung der falschen Daten zu erwirken. Zudem musste bereits nach bisherigem Recht zwingend Auskunft über Herkunft und Empfänger fehlerhafter Daten erteilt werden.

Mit der Änderung des § 34 BDSG soll das Auskunftsrecht allerdings gestärkt und erweitert werden. Dabei ist zu berücksichtigen, dass die Norm keine Darlegungslast der Betroffenen vorsieht. Diese haben nicht zu erläutern, aus welchen Gründen sie eine Auskunft (über Herkunft und Empfänger) begehren. Solange die Auskunftei daher nicht stichhaltig begründen kann, weshalb im Einzelfall das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegen soll, geht die Abwägung **zugunsten** des Interesses **der auskunftsbegehrenden Person** an einer **vollständigen Auskunft** aus. Eine Einschränkung des Auskunftsrechts kann auch nicht allein damit begründet werden, dass in den jeweiligen Verträgen zwischen Auskunfteien und deren Vertragspartnern und -partnerinnen die Geschäftsbeziehung als Geschäftsgeheimnis bezeichnet wird. Hierfür müssen besondere, objektiv nachprüfbare Umstände vorliegen, da ansonsten die Gesetzesänderung weitgehend leer liefe.

Die Verwirklichung der Auskunftsrechte der Betroffenen ist von den Auskunfteien unverzüglich umzusetzen.

8.4.2 Scoringverfahren der SCHUFA

Für Irritationen bei Bürgerinnen und Bürgern sorgt immer wieder das Scoringverfahren der SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung). Dabei geht es im Wesentlichen um Folgendes:

Die SCHUFA bietet ein so genanntes **Scoringverfahren** an, mit dem eine Prognose über das zukünftige Zahlungsverhalten einer Person getroffen wird. Der Düsseldorfer Kreis als Gremium der obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich geht ganz überwiegend von der Zulässigkeit des Verfahrens aus, auch wenn die datenschutzrechtliche Überprüfung noch nicht endgültig abgeschlossen ist.

Mit dem Scoringverfahren soll - so die Eigenwerbung der Auskunfteien - die Kreditwürdigkeit auch in Fällen beurteilt werden, in denen keine negativen Informationen über das Zahlungsverhalten einer Person in der Vergangenheit vorliegen. Anhand statistisch-mathematischer Methoden werden **Prognosen** über das **zukünftige Verhalten** von Personengruppen erstellt. Ausgedrückt wird die Prognose durch eine Punktzahl (**Score**), die zur Einordnung in eine bestimmte **Risikoklasse** führt. Hinsichtlich der Aussagekraft der Prognose ist zu berücksichtigen, dass alle Betroffenen - auch die mit schlechtem Scorewert - keinerlei Negativeintrag bei der SCHUFA haben und daher insoweit unbescholtene, kreditwürdige Personen sind.

Der Scorewert beschreibt als **Wahrscheinlichkeitsmerkmal** immer nur das Risiko für Kredite mit vergleichbaren Merkmalen zu einem bestimmten Zeitpunkt. Dabei gibt es für verschiedene Vertragsarten (beispielsweise Telekommunikationsvertrag, Bankkredit) unterschiedliche Berechnungsverfahren. Bei den in die Ermittlung des Scorewertes einfließenden Daten handelt es sich um zulässigerweise von der SCHUFA gespeicherte Informationen. Dazu gehören beispielsweise Angaben über die Anzahl noch ausstehender Ratenkredite, die Anzahl vorzeitig erledigter Kredite oder die Zahl der verschiedenen beauftragten Kreditinstitute. In die Berechnung des Scorewertes floss bis vor einiger Zeit ebenfalls die Anzahl der von den Betroffenen eingeholten **Selbstauskünfte** ein. Dies wurde von den Aufsichtsbehörden stets vehement kritisiert und führte letztendlich dazu, dass die SCHUFA sich bereit erklärte, hiervon Abstand zu nehmen. Die technische Umsetzung dieser Zusage wurde Mitte 2002 abgeschlossen.

Ein weiterer strittiger Punkt zwischen Aufsichtsbehörden und SCHUFA betraf die **Auskunftserteilung über den Scorewert** an die Betroffenen, die oft

mit den negativen Konsequenzen eines „schlechten" Scorewertes konfrontiert waren, ohne ihn erfahren zu können. Die SCHUFA stellte sich auf den Standpunkt, dass sie den übermittelten Scorewert nicht in eine Selbstauskunft einbeziehen könne, da er nicht gespeichert werde. Die gegenwärtig genutzte Software lasse eine Speicherung nicht zu. Die Aufsichtsbehörden regten an, diese Praxis aus Gründen der Transparenz gegenüber den Betroffen zu überdenken und waren mit der SCHUFA einig, dass die Vertragspartner der SCHUFA gehalten sind, soweit möglich den ihnen übermittelten Scorewert auf Anfrage mitzuteilen.

Nach intensiven Erörterungen zwischen den Aufsichtsbehörden und der SCHUFA erklärte sie sich außerdem dazu bereit, den Betroffenen eine **tagesaktuelle Scorewertberechnung** anzubieten. Diese Werte können jedoch von denjenigen abweichen, die zu früheren Zeitpunkten bereits an Dritte übermittelt wurden. Das Verfahren ist kostenpflichtig. Der Scorewert kann auch ohne eine umfassende Selbstauskunft erfragt werden. Für die nächste Softwaregeneration, die ab Ende 2003/Anfang 2004 in einem Pilotprojekt erprobt werden soll, plant die SCHUFA, die Speicherung des Scorewertes zu ermöglichen.

Im Zusammenhang mit den geschilderten Verhandlungen über die Auskunftserteilung des Scorewertes konnten die Aufsichtsbehörden erreichen, dass die SCHUFA nunmehr den Betroffenen die Möglichkeit einräumt, **Widerspruch gegen die Scorewertermittlung** einzulegen. Der Widerspruch muss nicht begründet werden. Allerdings informiert die SCHUFA den Betroffenen nach Einlegung des Widerspruchs noch einmal über mögliche Folgen einer Nichtermittlung des Scorewertes. Nur wenn der Betroffene auf dieses Schreiben hin seinen Widerspruch aufrecht erhält, sieht die SCHUFA zukünftig von einer Scorewertermittlung ab. Folgen danach weitere Anfragen zum Scorewert, übermittelt die SCHUFA Auskünfte mit folgendem Text: „Betroffener widerspricht Scoreberechnung. Über angefragte Person erfolgt keine Scoreermittlung".

Kritisch an dieser Verfahrensweise ist, dass Betroffene faktisch zweimal Widerspruch erheben müssen und zudem in der Auskunft der Widerspruch erwähnt wird. Zu begrüßen ist jedoch die Möglichkeit, eine Scorewertermittlung ganz zu unterbinden.

Insgesamt haben die bisherigen Verhandlungen der Aufsichtsbehörden mit der SCHUFA zum Scoreverfahren einige Fortschritte für die Betroffenen erbracht.

8.4.3 Zeitdauer der Auskunft: „Bestrittene Daten in Prüfung"

Wird die Richtigkeit der Datenbestände von Auskunfteien, wie etwa der SCHUFA, von den Betroffenen bestritten, sind die Daten, sofern die speichernde Stelle die Richtigkeit der gespeicherten Daten nicht nachweisen kann, nach § 35 Abs. 4 BDSG zu sperren.

Während der Feststellungsfrist, in der die Richtigkeit geprüft wird, gibt die SCHUFA nur die Auskunft „**Bestrittene Daten in Prüfung**". Der Hinweis erfüllt aus Sicht der Aufsichtsbehörden jedoch nicht die Anforderungen an eine Sperrung, wie sie das BDSG in §§ 35 Abs. 4, 3 Abs. 4 Nr. 4 vorschreibt. Danach dürfen grundsätzlich weder gesperrte Daten noch ein solcher Hinweis übermittelt werden. Diese Problematik ist seit längerer Zeit Gegenstand einer gemeinsamen Diskussion mit den Verantwortlichen der SCHUFA. Durch den Hinweis der SCHUFA wird indirekt das Bestehen einer, wenngleich umstrittenen, Forderung gegen die Betroffenen offenbart. Er kann bewirken, dass die Empfängerinnen und Empfänger Vermutungen zum Nachteil der Betroffenen anstellen. Etwa im Zusammenhang mit einer Kreditvergabe wird dann möglicherweise zu Lasten der Betroffenen eine ungünstigere Entscheidung getroffen als dies bei einer ordnungsgemäßen Sperrung und Beauskunftung ohne den Hinweis der Fall gewesen wäre.

Die Aufsichtsbehörden vertreten daher übereinstimmend die Auffassung, dass der Hinweis „Bestrittene Daten in Prüfung" nur für einen eng begrenzten Zeitraum - **maximal zwei Wochen** - beauskunftet werden darf. Lässt sich der umstrittene Sachverhalt innerhalb dieser Frist nicht aufklären, muss eine **Sperrung im Sinne des § 35 Abs. 4 BDSG** vorgenommen werden mit der Folge, dass spätere Auskünfte auch keinerlei Hinweis auf die Tatsache der Sperrung enthalten dürfen.

8.4.4 Nachbarschaftsbefragungen

Auskunfteien setzen in Einzelfällen Nachbarschaftsbefragungen als Mittel ein, um die Richtigkeit bereits gespeicherter Daten „zu überprüfen" oder um weitere Informationen über den Betroffenen zu sammeln. Nachbarschaftsbefragungen sind grundsätzlich unzulässig.

Die Unzulässigkeit folgt aus § 4 Abs. 2 BDSG, wonach personenbezogene Daten generell bei der entsprechenden **Person selbst zu erheben** sind. Nur wenn eine Person trotz wiederholter Versuche persönlich nicht zu erreichen

ist, darf in der Nachbarschaft danach gefragt werden, ob sie sich noch unter der genannten Anschrift aufhält. Eine solche ausnahmsweise zulässige Nachbarschaftsbefragung hat sich auf die **Feststellung des Wohnortes** der Betroffenen zu beschränken. Darüber hinausgehende Informationen dürfen **nicht erhoben** oder gespeichert werden. Dies gilt auch dann, wenn Nachbarinnen oder Nachbarn zusätzliche Angaben über die Betroffenen ungefragt offenbaren. Werden auf diesem Wege im Einzelfall gleichwohl andere als die Adressdaten erhoben oder gespeichert, kann dies als Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG mit einer Geldbuße bis zu 250.000 € geahndet werden.

Stellen Betroffene fest, dass die Nachbarschaft zu ihrer Person befragt wurde, sollten sie sich an die verantwortliche Stelle wenden und **Auskunft** über die dort gespeicherten Daten und deren Herkunft verlangen. Wurden aufgrund der Nachbarschaftsbefragungen über die Anschrift hinausgehende Daten gespeichert, sind diese nach § 35 Abs. 2 Nr. 1 BDSG umgehend zu löschen.

In den entsprechenden Fällen wurden die Auskunfteien auf die engen Grenzen einer zulässigen Nachbarschaftsbefragung hingewiesen.

8.4.5 Vom mittelalterlichen Marktplatz ins Internet: Pranger- und Warndateien

Neue technische Möglichkeiten schaffen neue Geschäftsideen; dabei werden oft alte Instrumente in neuer Form wiederbelebt. Ein gutes Beispiel dafür sind in den letzten Jahren sprunghaft gestiegene Versuche, Internetpranger und Internet-Warndateien einzurichten.

Die Frage vieler Unternehmen, wie zahlungskräftig ihre (potentiellen) Kundinnen und Kunden sind, gewinnt in unserer Informationsgesellschaft stetig an Bedeutung. Mit der Entwicklung vom anonymen Barkauf zum personalisierten bargeldlosen Kreditkauf - innerhalb oder außerhalb des Internet - entsteht eine wachsende Nachfrage nach **Bonitätsinformationen**. Diese werden von Online-Auskunfteien und Internet-Warndateien angeboten. In Sekundenschnelle können Unternehmen per Knopfdruck automatisiert vielfältige Auskünfte über die Kreditwürdigkeit ihrer potentiellen (online-) Kundinnen und Kunden abrufen. Auch die derzeitige wirtschaftliche Situation verstärkt das Bedürfnis, sich vor zahlungsunfähigen oder -unwilligen Kundinnen und Kunden zu schützen.

Das Internet lässt mehr und mehr Unternehmensgründerinnen und -gründer vom Aufbau einer eigenen Online-Warndatei träumen. Besonders bedenklich ist, dass einige Geschäftsleute eine mittelalterliche Praxis wieder einführen wollen: Schuldnerinnen und Schuldner sollen - datenschutzwidrig - öffentlich angeprangert werden. Nur steht der Pranger nicht mehr auf dem städtischen, sondern auf dem weltweiten virtuellen Marktplatz, im Internet. Einmal - aus welchen Gründen auch immer - an den **Internetpranger** gestellt, kann die diskriminierende personenbezogene Information weltweit abgerufen werden und ist - wegen möglicher downloads - nicht mehr sicher rückholbar.

Auch in Nordrhein-Westfalen wollten im Berichtszeitraum mehrere Unternehmen eine Prangerseite im Internet einrichten. Nachdem sie über die datenschutzrechtliche **Unzulässigkeit** des Vorhabens unterrichtet wurden, gaben sie ihre Geschäftsidee auf. Der moderne Pranger ist unter anderem schon deshalb nicht mit dem BDSG vereinbar, weil die ins Internet gestellten Daten für alle abrufbar wären, also auch für diejenigen, die kein berechtigtes Interesse an den Informationen haben.

Einige Gründerinnen und Gründer haben ihre Idee deshalb modifiziert. Sie wollen nun für einen **geschlossenen Kreis** von Benutzerinnen und Benutzern - meistens Unternehmen einer bestimmten Branche - eine Internet gestützte **Auskunftei** beziehungsweise Warndatei einrichten. Die Vertragspartnerinnen und -partner sollen bonitätsrelevante Informationen über die Personen abrufen können, die mit ihnen Verträge (mit Ausfallrisiko) abschließen wollen. Dabei sind allerdings sehr **strenge** datenschutzrechtliche **Anforderungen** zu beachten: So dürfen ohne Einwilligung der Betroffenen nur so genannte „harte Negativmerkmale" in die Datei gemeldet werden. **„Harte Negativmerkmale"** sind beispielsweise Vollstreckungsbescheide, rechtskräftige Urteile und eidesstattliche Versicherungen. Erfolglose Mahnungen oder der Hinweis auf eine „schlechte Zahlungsmoral" reichen keineswegs aus, um Daten von Schuldnerinnen und Schuldnern in einer Warndatei oder Auskunftei zu speichern. Die Abrufenden sind zudem verpflichtet, für jeden einzelnen Abruf ihr **berechtigtes Interesse** an den Daten glaubhaft zu machen. Ein berechtigtes Interesse liegt insbesondere dann vor, wenn zwischen der abrufenden und der eingemeldeten Person ein Vertragsabschluss unmittelbar bevor steht und die oder der Abrufende dabei ein **Ausfallrisiko** trägt, weil beispielsweise gegen Rechnung geliefert oder geleistet wird. Die Internet-Auskunftei hat die von den Abrufenden dargelegten Gründe für das berechtigte Interesse stichprobenartig zu überprüfen. Um das zu ermöglichen,

müssen die Abrufenden die entsprechenden **Gründe** und Nachweise **aufzeichnen**.

Darüber hinaus sind unter anderem **zu beachten**: Löschungs-, Benachrichtigungs- und Schadensersatzpflichten, die Auskunftsrechte der Betroffenen, technische und organisatorische Anforderungen an die Datensicherheit sowie die Pflicht der zwingend zu bestellenden betrieblichen Datenschutzbeauftragten, das gesamte Vorhaben vorab auf die Vereinbarkeit mit dem Datenschutz hin zu prüfen.

Alles in allem gilt: Um eine Warndatei im Internet oder eine Online-Auskunftei zu betreiben, braucht es nicht nur technisches Know-how und wirtschaftliches Geschick, sondern vor allem auch professionelle Kenntnisse des Datenschutzrechts.

8.5 Kreditwirtschaft

8.5.1 Auswertung des Überweisungsverkehrs zu Werbezwecken

Manche Kreditinstitute haben Kontenbewegungen ausgewertet, um Kundinnen und Kunden zielgerichtet Versicherungsangebote zu unterbreiten.

Bereits im 13. Datenschutzbericht 1995/96 unter 19.4, S. 120 wurde darauf hingewiesen, dass Daten von Kundinnen und Kunden nur dann für Angebote genutzt werden dürfen, wenn hierzu vorher deren ausdrückliche **Einwilligung** eingeholt wurde. Aus Kontobewegungen lassen sich viele Erkenntnisse über die Lebensumstände der Kontoinhaberinnen und -inhaber gewinnen, beispielsweise Arztrechnungen, Unterhaltszahlungen, hohe Lebensversicherungsbeiträge. Schon wegen der Vielzahl der hier anfallenden Daten und der nahezu unbegrenzten **Auswertungsmöglichkeiten**, die sich bieten, kommt es für die schutzwürdigen Belange der Betroffenen nicht entscheidend darauf an, ob ein mehr oder weniger sensibles Datum zur Auswertung herangezogen wird oder dieses auch anderen Personen bekannt ist oder nicht.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind einhellig der Auffassung, dass einer **Auswertung des Überweisungs- und Zahlungsverkehrs** von Kontoinhaberinnen und -inhabern **zu Werbe- und Akquisitionszwecken** überwiegende schutzwürdige Belange der

Betroffenen entgegen stehen, so dass § 28 Abs. 1 BDSG nicht als Erlaubnisnorm hierfür herangezogen werden kann.

Die betroffenen Kreditinstitute wurden nachdrücklich aufgefordert, ihr unzulässiges Verhalten zu beenden und zukünftig weder im Einzelfall noch systematisch den Zahlungs- und Überweisungsverkehr auszuwerten, um dies zur Werbung für andere Produkte zu nutzen.

8.5.2 Absenkung des Schwellenbetrages nach dem Geldwäschegesetz in der Euro-Umtauschphase

Mit dem Geldwäschegesetz (GwG) soll die organisierte Kriminalität und deren Folgen bekämpft werden. Das GwG verpflichtet insbesondere Kreditinstitute, ihre Kundinnen und Kunden bei bestimmten Bankgeschäften zu identifizieren und die entsprechenden Angaben aufzuzeichnen und aufzubewahren.

Derzeit liegt der Schwellenbetrag, der eine allgemeine **Identifizierung** der einzahlenden Person bei der Durchführung bestimmter Finanztransaktionen erforderlich macht, bei 15.000 €. Identifizieren ist nach § 1 Abs. 5 GwG „das Feststellen des Namens aufgrund eines **Personalausweises** oder **Reisepasses** sowie des Geburtsdatums und der Anschrift, soweit sie darin enthalten sind, und das Feststellen von Art, Nummer und ausstellender Behörde des amtlichen Ausweises".

Anlässlich von Beschwerden stellte sich heraus, dass ein Kreditinstitut für den Zeitraum vom 01.12.2001 bis 28.02.2002 (Euro-Umtauschphase) den Schwellenbetrag nach dem GwG aufgrund einer Entscheidung der Geschäftsleitung bankintern auf 5.000 € absenkte mit der Folge, dass bereits bei Ein- oder Auszahlungen ab diesem Betrag eine Identifizierung nach dem GwG durchgeführt wurde. Diese Daten wurden in einem eigens dafür vorgesehenen Datenbankprogramm gespeichert.

Aus den Regelungen des GwG ergibt sich, dass bei **Unterschreiten des Schwellenbetrages** eine Identifizierung nur zulässig ist, wenn begründete Tatsachen vorliegen, die auf eine erkennbar künstliche Aufsplittung der Finanztransaktion (so genanntes smurfing) hinweisen. Eine solche Verdachtslage kann jedoch nicht allein mit der Euro-Umtauschphase begründet und auf alle Kundinnen und Kunden bezogen werden. Nur wenn Tatsachen festgestellt worden sind, die darauf schließen lassen, dass die vereinbarte Transaktion den Geldwäschetatbestand des § 261 Straf-

gesetzbuch (StGB) erfüllt, ist eine Identifizierung unterhalb der genannten 15.000 € möglich. Selbst das betroffene Kreditinstitut verneinte das Vorliegen einer solchen Verdachtslage, zumal diese Verdachtslage **einzelfallbezogen** geprüft werden muss.

Da die Datenerhebung somit unzulässig war, wurde das Kreditinstitut aufgefordert, die so gewonnenen Daten zu löschen, was dann auch geschah.

9 Beschäftigte und Arbeitsorganisation

Da immer noch kein Entwurf eines **Arbeitnehmerdatenschutzgesetzes** vorliegt (15. Datenschutzbericht 2001 unter 15., S. 126), sind weiterhin auf die Verarbeitung von Beschäftigtendaten in Arbeitsverhältnissen im nicht-öffentlichen Bereich im Wesentlichen die §§ 28, 31, 33, 34, 35 und 39 BDSG anzuwenden. Diese Bestimmungen erweisen sich zunehmend als unzureichend für die Gewährleistung des auch auf den Bereich der Privatwirtschaft ausstrahlenden Rechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer.

So beklagten beispielsweise zahlreiche Arbeitssuchende immer wieder den nachlässigen Umgang der angeschriebenen Unternehmen mit ihren **Bewerbungsunterlagen**. Hier gilt: Unterlagen von Bewerbungen, die nicht zu einer Einstellung geführt haben, sind unverzüglich den Betroffenen zurückzusenden. Ihre Rückgabe ist notfalls einklagbar. Weiterhin ist zu beachten, dass nur autorisierte Beschäftigte Zugang zu Bewerbungsunterlagen haben. Diese Unterlagen sind entsprechend zu sichern.

Weiter gab es verschiedene Fragen zur **Privatpost** an Büroadressen. Hier sollte der Absender zuvor darauf hingewiesen werden, unter dem Namen der Empfängerin oder des Empfängers den Zusatz „Persönlich" zu verwenden. Allerdings schützt auch ein solcher Zusatz nicht gänzlich vor einem Öffnen „aus Versehen".

9.1 Dienstliche und private Nutzung von E-Mail und Internet am Arbeitsplatz

Zahlreiche Anfragen beziehen sich auf die dienstliche und private Nutzung von E-Mail und Internet am Arbeitsplatz. Die Problemfelder reichen von der Protokollierung der Nutzungsdaten, über Virenscannen bis hin zur Einsichtnahme von E-Mails durch Arbeitgeberinnen und Arbeitgeber.

Anfragende Personen waren sowohl Arbeitnehmerinnen und Arbeitnehmer als auch Personal- beziehungsweise Betriebsräte und Arbeitgeberinnen und Arbeitgeber. In vielen Fällen wurde aufgrund der gegebenen Hinweise eine neue, datenschutzrechtlich verbesserte **Dienstanweisung** oder **Betriebsvereinbarung** verfasst, die zu den nachfolgenden Schwerpunkten Regelungen treffen sollte:

Dienstliche Nutzung

Gestatten die Arbeitgeberinnen und Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, so stellt dies gegenüber den Beschäftigten **kein Diensteangebot** im Sinne des Telekommunikations- oder Teledienstrechts dar. Die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamten- oder Arbeitsrechts beziehungsweise der Landesdatenschutzgesetze oder des BDSG. Arbeitgeberinnen und Arbeitgeber haben grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen oder das Versenden von E-Mails dienstlicher Natur ist. Eine automatisierte Vollkontrolle ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten zu sehen und daher nicht erlaubt. Hingegen ist eine **Kontrolle** bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat oder dem Betriebsrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren **protokolliert** wird, dürfen diese Daten ausschließlich zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

Private Nutzung

Wird den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, so liegt ein Telekommunikations- beziehungsweise Teledienstangebot vor. Hier gilt es, das Telekommunikationsgesetz, die Telekommunikations-Datenschutzverordnung und das Teledienstedatenschutzgesetz einzuhalten.

Die Beschäftigten haben **keinen Anspruch** auf eine private Nutzung des Internet. Wird jedoch eine private Nutzung erlaubt, so ist es grundsätzlich möglich, diese Erlaubnis an **einschränkende Voraussetzungen** zu knüpfen (zum Beispiel eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die solche Voraussetzungen nicht erfüllen wollen, müssen ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern können. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der

Kontrolle, ob diese Bedingungen eingehalten werden, müssen - am sinnvollsten durch **Dienst-** oder **Betriebsvereinbarung** - eindeutig geregelt werden. Eine Protokollierung darf ohne Einwilligung nur erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

Für die private E-Mail gilt, dass sie wie **private schriftliche Post** zu behandeln ist. Das Telekommunikationsgeheimnis ist zu wahren. Soweit für Mitarbeiterinnen und Mitarbeiter keine separaten privaten E-Mail-Accounts eingerichtet werden, was der Regelfall sein wird, müssen bei Kontrollen mitprotokollierte Inhalte, sobald ein privater Charakter erkannt wird, von der weiteren Betrachtung ausgeschlossen werden.

Einsatz von Virenscanprogrammen

Der Einsatz von Virenscanprogrammen ist entgegen der Befürchtung mancher Bürgerinnen und Bürger in der Regel unproblematisch. Dies gilt insbesondere, wenn die Nutzung eines Mailsystems nur zum dienstlichen Gebrauch gestattet ist. Die **automatisierte** Prüfung von eingehenden Mails auf Viren ist sogar aus Datenschutz- und Datensicherheitsgründen notwendig, da nur mittels solcher Instrumente betriebsinterne Netze, und damit auch Dateien mit personenbezogenen Daten, gegen Angriffe von außen durch Viren, Würmer und Trojanische Pferde geschützt werden können. Sie gehören somit zu den allgemeinen **technischen Schutzmaßnahmen**, deren präventive Wirkung gerade den Einsatz repressiver Mittel wie die personenbezogene Überwachung entbehrlich machen soll.

Beim Einsatz von Virenscanprogrammen ist zu beachten, dass die damit einhergehenden **organisatorischen Regelungen** im Sinne des Datenschutzes gefasst werden. Es sind Produkte einzusetzen, die einen automatischen, zunächst anonymen Scan-Vorgang durchführen. Die Beschäftigten sind mittels Dienst- oder Betriebsvereinbarung darüber zu unterrichten, welche Daten im Rahmen eines Scan-Vorgangs gegebenenfalls erfasst werden und wie mit virenbehafteten Mails umgegangen wird.

Quittungsverfahren und Lesebestätigungen

Der Einsatz von Quittungsverfahren bei Mail-Produkten ist datenschutzrechtlich nicht zu beanstanden. Dies gilt insbesondere, soweit es sich um Post handelt, die an Dritte verschickt wird, also an nicht behörden- oder betriebszugehörige Personen. Hierbei handelt es sich um eine rein **organisatorische Maßnahme**, die durch die Leitung der Organisation bestimmt werden kann. Es bleibt der Leitung beispielsweise auch selbst überlassen, ob sie herkömmliche Post „normal", mit Einschreiben oder gar als Einschreiben mit Rückschein versendet. Zu beachten ist jedoch, dass eine automatische Lesebestätigung lediglich den Empfang beziehungsweise das Öffnen einer Mail bestätigt. Die Aussage, ob die Empfängerin oder der Empfänger auch Kenntnis von dem Inhalt genommen hat, kann mittels dieser Option ohnehin nicht getroffen werden.

Bei interner Nutzung von Mail-Systemen muss im Rahmen einer Betriebs- oder Dienstvereinbarung geregelt werden, dass die Zuschaltung von Quittungsverfahren und Lesebestätigungen nicht für eine Leistungs- oder Verhaltenskontrolle genutzt werden darf.

9.2 Überwachung am Arbeitsplatz

Mit der Übertragung der Zuständigkeit für die Datenschutzaufsicht im nicht-öffentlichen Bereich nahm die Zahl der Beschwerden sprunghaft zu, die das Thema Zugriffsrechte und Überwachung der Datenverarbeitung am Arbeitsplatz zum Inhalt hatten. Hauptsächlich wurden folgende Aspekte nachgefragt:

Zugriff durch unzureichendes Berechtigungskonzept

Grundsätzlich sind nach den Datenschutzgesetzen Datenverarbeitungssysteme, in denen personenbezogene Daten verarbeitet werden, so zu gestalten, dass eine unbefugte Speicherung sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten verhindert wird. Insbesondere ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Hierfür sind entsprechende technische und organisatorische Maßnahmen zu treffen. Es ist daher erforderlich, **Zugriffsrechte** so zu gestalten, dass erst nach **geeigneter Identifizierung**, die für die

Arbeit erforderlichen Datenbestände und Programme zur Verfügung gestellt werden. Gleichzeitig wird die Verantwortung für alle Transaktionen der freigegebenen Kennung zugerechnet.

Zugriff durch Vorgesetzte

Um Vorgesetzten den Zugriff auf die dem Verantwortungsbereich ihrer Mitarbeiterinnen und Mitarbeiter unterliegenden Daten zu ermöglichen, sind geeignete **Berechtigungskonzepte** zu erstellen, die die Weisungsbefugnisse widerspiegeln. Hierbei sollte auch die Sensibilität der Daten (beispielsweise Personaldaten) berücksichtigt werden. Dies gilt gleichermaßen für Vertretungsfälle.

Ein Voll- oder Lesezugriff auf die Datenverarbeitung der Mitarbeiterinnen und Mitarbeiter durch **Weitergabe der Passworte** an Weisungsberechtigte oder Vorgesetzte hat wegen der notwendigen Einhaltung der Datensicherheit grundsätzlich zu **unterbleiben**. Von einer effektiven Geheimhaltung der Passworte hängt ein wesentlicher Teil der Systemsicherheit ab (Authentizität, Revisionsfähigkeit). Die Mitarbeiterinnen und Mitarbeiter müssen daher verpflichtet sein, ihre Passworte nicht preiszugeben, auch nicht gegenüber ihren Vorgesetzten. Vorgesetzte sollten ihre Arbeit unter der **eigenen** und nicht unter fremder **Kennung** vornehmen, es sei denn, sie übernehmen die Verantwortung für die Transaktionen der Mitarbeiterinnen und Mitarbeiter und die Übernahme der Verantwortung wird verfälschungssicher zweifelsfrei dokumentiert. Anderenfalls hätten sie die Möglichkeit, unter fremder Kennung Daten zu verändern oder auch zu versenden, ohne in den entsprechenden Protokollen als Veranlassende der Datenänderung ausgewiesen zu werden.

Wird es den Mitarbeiterinnen und Mitarbeitern ausdrücklich erlaubt, DV-Systeme privat zu nutzen, müssen die privat erstellten Dateien vor dem Lesezugriff Dritter durch wirksame Mechanismen geschützt werden. Sie dürfen auch **nicht zu Kontroll- und Überwachungszwecken** durch Personal des Betriebes geöffnet, durchgesehen oder in sonstiger Weise verarbeitet werden.

Werden die betrieblichen DV-Systeme rein tatsächlich durch die Beschäftigten für private Zwecke genutzt, so müssen sich die Beschäftigten bewusst sein, dass ihre privaten Dateien in gleicher Weise dem Zugriff des Betriebes ausgesetzt sind wie ihre dienstlichen Dateien. Ohne ausdrückliche Erlaubnis des Betriebes, in der Regel in einer Betriebsvereinbarung enthalten, ist die Nutzung der betrieblichen DV-Ressourcen für **private**

Zwecke unzulässig. Inwieweit eine tatsächliche Duldung der privaten Nutzung durch den Betrieb vorliegt und gegebenenfalls zu einer anderen rechtlichen Bewertung führt, hängt von den Umständen des Einzelfalles ab.

Auswertung von Protokolldateien

Durch gezielte Auswertung der Protokollierung von Verarbeitungsaktivitäten können beispielsweise **Nutzungsprofile** der Mitarbeiterinnen und Mitarbeiter erstellt werden. Die allgemeinen Datenschutzbestimmungen lassen eine derartige Auswertung der Protokolldateien nicht zu. Daten von Beschäftigten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder der Sicherstellung des ordnungsgemäßen Betriebes gespeichert werden, dürfen **nicht für andere Zwecke** verarbeitet werden.

Zugriff durch die Systemadministration

Hier gilt es, die Allmacht der Systemadministration so zu beschränken, dass sie kontrollierbar bleibt. Das BDSG und DSG NRW verpflichten die Stellen aus Wirtschaft und Verwaltung, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die gewährleisten, dass nur **Befugte** personenbezogene Daten zur Kenntnis nehmen können (§ 9 BDSG, § 10 DSG NRW).

Einsatz von Netzwerkmanagement-/Remote-Administrations-Software

Die zurzeit auf dem Markt angebotenen Netzwerkmanagementtools verfügen in der Regel auch über Remote-Control und Remote-Access-Funktionen. Auch hier gilt es durch Einschränkung der Netzwerkadministrationsrechte (beispielsweise verteiltes Management) und durch Kontrolle der Administrationsaktivitäten einen Missbrauch insbesondere bei der Erschleichung von Systemrechten zu verhindern. Vor dem Einsatz von Netzwerkmanagementtools sollte ein **Sicherheitskonzept** erstellt werden, in dem alle Anforderungen an ein Netzwerkmanagement beschrieben sind. Insbesondere die Definition der Administrationsrechte sollte besonders sorgfältig erfolgen. Zusätzlich sollte aus Datensicherheitsgründen darauf geachtet werden, dass möglichst viele Funktionen wirksam überwacht und - soweit nicht dauerhaft benötigt - deaktiviert werden können.

Einsatz von speziellen Überwachungsprogrammen

Alarmierend sind die hohen Verkaufszahlen von so genannten Spionageprogrammen, die für die Überwachung von PC-Arbeitsplätzen in Betrieben und auch im häuslichen PC-Bereich eingesetzt werden können.

Derartige Überwachungsprogramme haben sich darauf spezialisiert, unbemerkt sämtliche **Nutzungsaktivitäten** wie beispielsweise Tastatureingaben oder Online-Aktivitäten zu **registrieren**. Der Einsatz derartiger Programme ist datenschutzrechtlich äußerst problematisch. Nur in besonders gelagerten Fällen - beispielsweise bei begründetem Missbrauchsverdacht - und nur unter Einhaltung genau definierter Bedingungen in Absprache mit dem Betriebsrat ist der Einsatz ausnahmsweise vertretbar. Alle Beschäftigten eines Betriebes sind unter Angabe des einzusetzenden Programms und unter transparenter Beschreibung möglicher Einsatzfälle und -situationen allgemein darüber zu unterrichten, dass der Betrieb beabsichtigt, möglicherweise bei Vorliegen der selbst definierten Voraussetzungen eine derartige „Spionagetätigkeit" gegen eigene Betriebsangehörige zu richten.

Außerdem muss auch die weitere Datenverarbeitung erläutert und **transparent** gemacht werden bis hin zu Zeitpunkt und Art der Löschung. Die Überwachung ist weiter so zu organisieren, dass jederzeit zweifelsfrei nachgewiesen werden kann, welcher Arbeitsplatz aus welchem konkreten Anlass, aufgrund welcher Entscheidung, wann, wie lange, in welchem Umfang überwacht wurde, wer Zugriff auf die so gewonnenen Daten und Erkenntnisse hatte, wer tatsächlich Zugriff genommen hat, an welche Personen oder Stellen welche Daten und Informationen übermittelt wurden und zu welchen Maßnahmen welche Daten konkret genutzt wurden.

Nach Abschluss der Überwachungsmaßnahme und vor der Löschung sind die Betroffenen jeweils von einer solchen Maßnahme zu unterrichten. Ihnen ist auf Wunsch Einsicht in die Unterlagen zu gewähren mit der Möglichkeit, Kopien anzufertigen oder anfertigen zu lassen, um ihre weiteren Rechte (beispielsweise auf Schadenersatz) wahrnehmen zu können. Ohne derartige **Vorkehrungen zur Wahrung der Rechte** der Betroffenen ist jede derartige Überwachungsmaßnahme rechtswidrig und unzulässig.

Wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz fordern daher auch die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 7./8. März 2002 den Bundesgesetzgeber auf, die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben (Abdruck im Anhang, Nr.15.).

9.3 Qualitätsmanagement bei der Polizei

Das Innenministerium hat einen Einführungserlass „Allgemeine Bürgerbefragung bei der Polizei NRW" vorbereitet. Dabei war zu berücksichtigen, dass die durch die Befragung gewonnenen Erkenntnisse einen Anfangsverdacht hätten begründen können, der zur Einleitung eines Ermittlungsverfahrens führen könnte, obgleich dies nicht Ziel und Zweck der Befragung sein sollte.

In diesem Erlass ist Bürgerzufriedenheit als ein wichtiges Organisationsziel der Polizei benannt worden. Es sind Vorgaben für alle Polizeibehörden und -einrichtungen gemacht worden, die diese jeweils dann in eigene Befragungen der Bürgerinnen und Bürger umsetzen sollten. Eine jährliche Berichtspflicht gegenüber dem Innenministerium ist dabei festgeschrieben.

Durch Versendung von Fragebogen mit einem Begleitschreiben sollten beispielsweise ebenso Erkenntnisse für eine effektive und bürgerorientierte Polizeiarbeit gewonnen werden wie auch durch eine direkte persönliche oder auch telefonische Befragung durch Polizeibeamtinnen und Polizeibeamte. Dabei hatte das Innenministerium unter dem Gesichtspunkt des **Mitarbeiterdatenschutzes** den Grundsatz aufgestellt, dass es unzulässig sei, Befragungsergebnisse, die durch die Art der Erhebung oder Auswertung (zum Beispiel bei Beschränkung des Befragungsgebietes auf den Bereich einzelner Organisationseinheiten) oder wegen geringer Personalstärke von Organisationseinheiten Rückschlüsse auf das Verhalten oder die Leistung einzelner Beschäftigter ermöglichen, für die Kontrolle persönlicher Ergebnisse zu nutzen.

Ein besonderes Datenschutzproblem ergab sich daraus, dass das Innenministerium entsprechend der grundlegenden Aufgabenstellung der Polizei festlegte, dass bei Vorliegen von aus der Befragung - insbesondere per Interview oder per Telefon - gewonnenen Erkenntnissen, die einen Anfangsverdacht begründen, diese zur **Einleitung eines Ermittlungsverfahrens zu nutzen** seien. Auf eine solche Zweckbestimmung der durch die Befragung erhobenen Daten wurden die zu befragenden Personen allerdings **nicht hingewiesen**. Da die als Befragungspersonen eingesetzten Polizeibeamtinnen und Polizeibeamten stets vor einer Befragung nicht wissen, ob die zu befragende Person einen Sachverhalt schildern wird, der geeignet ist oder sein könnte, einen Anfangsverdacht als Ausgangspunkt für ein polizeiliches Ermittlungsverfahren zu begründen, hätten alle Befragten vor Beginn der Befragung zumindest nach § 55 Abs. 2 Strafprozessordnung (StPO) belehrt

werden müssen. Dies hätte jedoch die Akzeptanz der Befragung deutlich gemindert. Das Innenministerium hat letztlich auf eine **persönliche oder telefonische Befragung** der Bürgerinnen und Bürger durch Polizeibeamtinnen und Polizeibeamte **verzichtet**.

Auch einer Reihe von anderen Datenschutzgesichtspunkten hat das Innenministerium bei der Ausgestaltung der Rahmenbedingungen für solche Bürgerbefragungen Rechnung getragen. So wurden beispielsweise **Warnhinweise** im Hinblick auf eine mögliche Selbstoffenbarung der schriftlich befragten Personen eingefügt.

Nach Überprüfung aller bekannt gewordenen Gesichtspunkte bestanden gegen die so formulierten Rahmenbedingungen für Befragungen von Bürgerinnen und Bürgern zur Zufriedenheit mit der Polizeiarbeit insgesamt keine durchgreifenden datenschutzrechtlichen Bedenken mehr. Datenschutzprobleme bei der Umsetzung dieser Empfehlungen des Innenministeriums in konkrete Befragungen einer Polizeibehörde vor Ort sind bisher nicht bekannt geworden.

9.4 Outsourcing der Beihilfe

Eine Verlagerung der Beihilfeabrechnung auf private Versicherungsunternehmen war und ist nach der geltenden Rechtslage unzulässig.

Allerdings beabsichtigt die Landesregierung, durch Änderung der **Beihilfeverordnung** den kommunalen Stellen zu ermöglichen, die Beihilfeabrechnung auf private Dritte zu übertragen. Auch dagegen sprechen folgende datenschutzrechtliche Gründe: Die Übertragung der Beihilfeabrechnung auf private Dritte beinhaltet eine Übermittlung personenbezogener **Gesundheitsdaten** der Betroffenen. Diese Weitergabe sensibler Beihilfedaten greift grundsätzlich in das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 des Grundgesetzes (GG) abgeleitete Recht auf informationelle Selbstbestimmung ein. Nach der Rechtsprechung des Bundesverfassungsgerichts sind Eingriffe in das informationelle Selbstbestimmungsrecht nur dann verfassungskonform, wenn sie auf Grund einer **gesetzlichen Grundlage** erfolgen (BVerfGE 65, 1 43; 92, 191 197). Der Eingriff, der mit der Weitergabe der sensiblen Beihilfedaten verbunden ist, bedarf somit einer Rechtsgrundlage.

Die Verordnungsermächtigung des Landes Nordrhein-Westfalen nach § 88 Satz 4 des Landesbeamtengesetzes (LBG) reicht jedoch für die Einrichtung einer regelmäßigen Datenübermittlung nicht aus. Modifikationen der beihilferechtlichen Verwaltungszuständigkeit sind zudem nur zugunsten von **Behörden** zulässig. Private Dritte müssten daher behördliche Eigenschaften aufweisen. Da jedoch eine Rechtspersönlichkeit des privaten Rechts nur dann über Behördeneigenschaft verfügt, wenn sie als **beliehene Unternehmerin** mit der Wahrnehmung einer Verwaltungsaufgabe betraut worden ist, kommt eine Übertragung auf private Dritte letztlich nur bei beliehenen Unternehmen in Betracht.

Neben einer rechtssatzmäßigen Deckung bedarf es somit auch eines Beleihungsaktes zugunsten privater Dritter. Nur auf diese Weise ist gewährleistet, dass die Bearbeitung der Beihilfeangelegenheiten Gegenstand des originären Aufgabenkreises der öffentlichen Stellen und damit derjenigen Stellen bleibt, die für das Wohl ihrer Beamtinnen und Beamten verantwortlich sind.

Überdies handelt es sich bei den Beihilfedaten um sensible **Personalaktendaten**. Diese Daten unterliegen als Bestandteile der Personalakten dem Personalaktengeheimnis. Eine Datenübermittlung an private Dritte würde dazu führen, dass behördenexterne Personen Zugang zu Personalakten oder deren Bestandteilen erlangen. Auf diese Weise würde zum einen das Personalaktengeheimnis, zum anderen auch § 102 Abs. 3 LBG unterlaufen, wonach der Zugang zu Personalakten nur solchen Beschäftigten des Dienstherrn vorbehalten ist, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Bereits aus dem Wortlaut dieser Vorschrift folgt, dass **behördenexternen Personen** der Zugang zu Personalakten von vornherein **verwehrt** ist. Die Konzentration des Personalaktenführungsrechts bei der Personalverwaltung soll gerade verhindern, dass Verwaltungsaufgaben, deren sachgerechte Wahrnehmung die Anlegung einer Personalakte notwendig voraussetzt (wie dies unter anderem bei der Beihilfesachbearbeitung der Fall ist), aus dem Internum der Personalverwaltung ausgelagert werden.

Abgesehen davon ist ohnehin fraglich, wie im Falle einer Übertragung der Beihilfeabrechnung auf private Dritte noch ein ausreichender Datenschutz gewährleistet werden kann. Dem Landesgesetzgeber dürfte überdies für die Festschreibung einer solchen Verpflichtung privater Stellen bereits die Gesetzgebungskompetenz fehlen, wenn der Bundesgesetzgeber mit dem

Bundesdatenschutzgesetz von der Gesetzgebungsbefugnis zur Datenverarbeitung Privater im Sinne des Art. 74 Abs. 1 Nr. 1 GG i.V.m. Art. 72 Abs. 1 GG entsprechend Gebrauch gemacht hat.

Abschließend bleibt festzuhalten, dass eine Änderung der Zuständigkeitsvorschriften der Beihilfeverordnung des Landes Nordrhein-Westfalen im Hinblick auf die Übertragung der Beihilfeabrechnung auf private Dritte unzulässig ist.

9.5 Datenschutz im Personalrat

Unabhängig von technischen und organisatorischen Vorkehrungen zur Sicherstellung des Datenschutzes bedarf es einer großen Sensibilität der Personalräte beim Umgang mit den ihnen anvertrauten Beschäftigtendaten im Spannungsfeld von allgemeiner Interessenvertretung und dem individuellen Recht auf informationelle Selbstbestimmung einzelner Beschäftigter.

Ein Personalrat hatte grundlegende Zweifel, ob der Umgang mit Daten von Beschäftigten, die ihm im Rahmen seiner Tätigkeit bekannt wurden, durch ihn als Institution und durch seine Mitglieder **datenschutzkonform gestaltet** war und hatte um einen Kontrollbesuch gebeten. Die vorgefundenen datenschutzrechtlichen Probleme in den Bereichen räumliche und technische Ausstattung des Personalrates, Aufbewahrung von Personalunterlagen mit Daten der Beschäftigten und Verfahren bei Vorlagen an den Personalrat konnten im Einvernehmen mit der Dienststelle und dem Personalrat erfolgreich behoben werden.

Die in diesem Verfahren und aus früheren Fällen (13. Datenschutzbericht 1995/1996 unter 17.3, S. 113 f.) gewonnenen Erkenntnisse fanden Eingang in die „Orientierungshilfe Datenschutz im Personalrat", die unter www.lfd.nrw.de im Internet abgerufen werden kann.

10 Vereine

10.1 Veröffentlichung von Mitgliederdaten im Internet

Die inzwischen weite Verbreitung des Internet führt auch bei Vereinen dazu, dass sie die Möglichkeiten dieses Mediums verstärkt nutzen. Dazu gehört auch die Veröffentlichung von Mitgliederdaten. Dementsprechend steigen die Anfragen von Mitgliedern zu diesem Themenkomplex.

Fraglos bietet das Internet Vereinen ein hervorragendes Forum zur Selbstdarstellung und Öffentlichkeitsarbeit. Soweit jedoch die Veröffentlichung personenbezogener Daten von Mitgliedern beabsichtigt ist, sollte aber eine sorgfältige Abwägung darüber stattfinden, in welchem **Umfang** dies für die damit verfolgten Zwecke **tatsächlich erforderlich ist**. Denn neben den Chancen des Internet müssen auch dessen **Risiken** berücksichtigt werden. Dazu zählt neben zahlreichen Fragen der Internetsicherheit die Tatsache, dass der Adressatenkreis unbegrenzt ist und einmal eingestellte Daten unkontrollierbar preisgegeben sind.

Deshalb ist für die Veröffentlichung personenbezogener Informationen über Vereinsmitglieder deren vorherige **schriftliche Einwilligung** erforderlich. Bei neu eintretenden Mitgliedern empfiehlt es sich, bereits bei der Datenerhebung für die Mitgliedschaft die Einwilligung einzuholen. Dabei ist darauf zu achten, dass den Betroffenen klar ist, welche Daten zur Veröffentlichung bestimmt sind und dass sie deren Umfang beschränken können. Ebenso ist auf die **Freiwilligkeit** der Erklärung und ihre jederzeitige **Widerruflichkeit** hinzuweisen. Bei Altmitgliedern bietet es sich an, über die Vereinsmitteilungen eine allgemeine Information, die die genannten Punkte berücksichtigt, mit einer zurückzusendenden Zustimmungserklärung zu verteilen.

Das Muster einer Einwilligungserklärung und weitere Informationen sind unter www.lfd.nrw.de zu finden und in dem Faltblatt „Datenschutz im Verein", das bestellt werden kann.

10.2 Übermittlung von Mitgliederdaten an Sponsoren

Auch jenseits von Champions League, Formel 1 und Tour de France, im so genannten Breitensport - dort wo Sport Spaß & Fitness und nicht Profit bringen soll - gewinnt das Sponsoring zunehmend an Bedeutung.

Als Gegenleistung für die finanzielle Unterstützung eines Vereins verlangen die Sponsoren häufig die Herausgabe von Mitgliederdaten, um diese für Werbezwecke nutzen zu können. Verstärkt fragen Vereinsmitglieder und Vereinsvorstände, ob das mit dem Datenschutz vereinbar ist oder wie die Zusammenarbeit datenschutzrechtskonform gestaltet werden kann.

Die **Weitergabe** (juristisch: Übermittlung) von Mitgliederdaten an einen Sponsor ist vom **Vereinszweck nicht gedeckt** und daher auch datenschutzrechtlich bedenklich. Deswegen empfiehlt es sich, die Zusammenarbeit mit dem Sponsor und die sich daraus ergebenden Konsequenzen auf einer Mitgliederversammlung zu erörtern und einen entsprechenden Beschluss herbeizuführen.

Eine Datenweitergabe an den Sponsor ist im Allgemeinen nur zulässig, wenn eine ausdrückliche **Einwilligung** des jeweiligen Mitglieds vorliegt. Vor allem bei Konstellationen, in denen die Tatsache der Mitgliedschaft als solche bereits Aufschluss über besonders schutzbedürftige Daten wie gesundheitliche Verhältnisse, politische oder religiöse Auffassungen gibt, dürfen Mitgliederdaten nur unter dieser Voraussetzung an Dritte übermittelt werden. Beispiele hierfür sind Suchtselbsthilfegruppen, Gewerkschaften, Elterninitiativen verhaltensauffälliger Kinder und dergleichen mehr.

Ansonsten gilt: Nur wenn **schutzwürdige Interessen** von Vereinsmitgliedern nicht entgegenstehen, kann der Verein dem Sponsor zu Werbezwecken bestimmte Daten - Name, Anschrift, akademische Grade, Titel und oder Geburtsjahr - auch ohne Einwilligung mitteilen (siehe hierzu unter 8.3.1). Zu beachten ist, dass Vereine im besonderen Maße verpflichtet sind, auf die schutzwürdigen Belange ihrer Mitglieder Rücksicht zu nehmen. Je nach Art des Vereins ist diesen Belangen ein unterschiedliches Gewicht beizumessen. So vertrauen insbesondere Mitglieder örtlicher Vereine regelmäßig darauf, dass der Verein ihre Daten grundsätzlich nicht für vereinsfremde Zwecke verwendet.

Entscheidet sich die Mitgliederversammlung für die Weitergabe der oben genannten Datenarten ohne Einwilligung, sollte der Vorstand alle Mitglieder darüber **unterrichten** und jedem einzelnen Mitglied die Möglichkeit einräumen, der Weitergabe der eigenen Daten zu **widersprechen**. Neue Mitglieder sind bei Eintritt in den Verein darüber zu informieren, welche Daten (zum Beispiel Name, Anschrift) zu welchem Zweck an den Sponsor weitergegeben werden. Auch sie sollten von Beginn an auf ihr

Widerspruchsrecht hingewiesen werden. Wichtig ist weiterhin, den Sponsor zu verpflichten, die Daten nur zu dem **vereinbarten Zweck** zu nutzen. Der Sponsor darf die Mitgliederdaten nicht für andere Zwecke nutzen oder gar an Dritte weitergegeben. Dies kann mit einer **Vertragsstrafenregelung** abgesichert werden.

Mehr Informationen zum Datenschutz im Verein finden Sie auf unserer Internetseite unter www.lfd.nrw.de und in dem Faltblatt „Datenschutz im Verein", das bestellt werden kann.

11 Bildung und Forschung

11.1 Schulen ans Netz

„Wir sind drin" - alle nordrhein-westfälischen Schulen verfügen inzwischen über einen Internetzugang. Bis Ende 2004 sollen alle Klassen mit Computern ausgestattet sein. Mit der Intensivierung des Interneteinsatzes steigt allerdings auch die Zahl der Eingaben zum Thema Datenschutz und Datensicherheit in den Schulen.

Die Chancen, die die Nutzung des Internet auch und gerade in der Schule bietet, sind unbestritten. Die damit einhergehenden **Risiken** des Surfens, Chattens und Mailens im Netz werden allerdings gerne verdrängt und Fragen zum datenschutzgerechten und sicheren Umgang mit dem Medium Internet oftmals erst gestellt, wenn bereits Fehler aufgetreten sind.

Antworten auf häufig gestellte Fragen und darüber hinausgehende Tipps, um unnötige Crashs auf der Schul-Datenautobahn möglichst bereits im Vorfeld zu vermeiden, gibt die **Orientierungshilfe „Schulen ans Netz"**, die bei der Dienststelle angefordert oder unter www.lfd.nrw.de abgerufen werden kann. Hier finden sich Hinweise zur technischen Absicherung und zur Internetnutzung innerhalb sowie außerhalb des Unterrichts, Ratschläge zur datenschutzgerechten Gestaltung der Schulhomepage und Vorschläge für eine schulinterne Nutzungsordnung.

Eine solche Orientierungshilfe kann allerdings immer nur eine Momentaufnahme tatsächlicher und rechtlicher Probleme sein, und auch seit der Veröffentlichung von „Schulen ans Netz" ist die Zeit natürlich nicht stehen geblieben. Eine neue Rechtslage ist durch das zwischenzeitlich in Kraft getretene **Informationsfreiheitsgesetz (IFG NRW)** und insbesondere durch die in ihm normierten Veröffentlichungspflichten entstanden (hierzu im Einzelnen unter 22.6). Das IFG NRW gilt für die öffentlichen Schulen.

Durften vormals Daten von Lehrerinnen und Lehrern regelmäßig nur mit deren Einwilligung und nur dann ausnahmsweise ohne Einwilligung auf der Schulhomepage veröffentlicht werden, wenn dies zur Aufrechterhaltung des Dienstbetriebs erforderlich war, hat sich dieses Regel-Ausnahme-Verhältnis mit In-Kraft-Treten des IFG NRW umgekehrt: Aus Gründen der **Transparenz** sind nunmehr Übersichten über Aufgaben- und Funktionszuweisungen innerhalb des Lehrerkollegiums grundsätzlich zu veröffentlichen, wenn der Veröffentlichung nicht im Einzelfall

ausnahmsweise - eng auszulegende -schutzwürdige Belange einer betroffenen Lehrerin oder eines betroffenen Lehrers entgegenstehen. Die **Veröffentlichung** kann - soweit möglich - elektronisch erfolgen und zwar mit Vor- und Familiennamen, Titel, akademischem Grad, Berufs- und Funktionsbezeichnung und gegebenenfalls dienstlicher Erreichbarkeit über Telefon sowie E-Mail, ohne dass es hierzu einer Einwilligung der Betroffenen bedarf. Neben den vorgenannten Daten des Lehrerkollegiums könnten beispielsweise auch die Stundenpläne mit den jeweils unterrichtenden Lehrkräften veröffentlicht werden. Fotos einer Lehrkraft dürfen allerdings im Hinblick auf ihr Recht am eigenen Bild auch weiterhin nur mit ihrer vorherigen wirksamen Einwilligung ins Netz gestellt werden.

11.2 Modell „Selbständige Schule" - aber bitte ohne Fiasko für den Datenschutz

Jede der 237 am Modellprojekt teilnehmenden Schulen hat künftig eigenverantwortlich eine Reihe von Entscheidungen zu treffen; gefordert sind insbesondere die Schulleitungen. Die Stärkung der Eigenverantwortlichkeit der Schulen ist zu begrüßen, wenn und soweit dem Datenschutz dabei hinreichend Rechnung getragen wird.

Mit der Öffnungsklausel in Art. 1 des Schulentwicklungsgesetzes vom 27. November 2001 sollen die an dem Modellvorhaben teilnehmenden Schulen abweichend von den bestehenden Rechtsvorschriften größere Selbständigkeit und Eigenverantwortung in personellen, finanziellen, organisatorischen und curricularen Fragen erhalten. Die in §§ 3 bis 5 der Verordnung „**Selbständige Schule**" - VOSS - vom 12. April 2002 getroffenen abweichenden Regelungen werden erhebliche Auswirkungen auf die Verarbeitung personenbezogener Daten - besonders in dem sensiblen Bereich der Personaldatenverarbeitung - zur Folge haben. Deswegen wurde das Schulministerium darauf hingewiesen, dass für die ausgewählten Schulen Datenschutzbeauftragte nach § 32a DSG NRW bestellt sein müssen.

Die notwendige Anpassung der Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer (VO-DV II) an die neuen Aufgabenstellungen ist leider noch nicht erfolgt, obwohl die Kooperationsverträge mit den ausgewählten Schulen bereits abgeschlossen sind. Datenschutzrechtliche Bestimmungen sind besonders in dem Bereich der Verarbeitung von Daten der Lehrkräfte in der Schule und bei den Schulaufsichts-

behörden, der Weitergabe solcher Daten an den Lehrerrat als dem personalvertretungsrechtlichen Organ sowie an Schulmitwirkungsorgane neu festzulegen.

Die Wahrnehmung neuer Aufgaben durch die Schulen darf in der Praxis nicht mit Einbußen für den Schutz der Beschäftigtendaten vonstatten gehen, insbesondere bei der schulinternen Personalaktenführung.

11.3 Information an Eltern volljähriger Schülerinnen und Schüler

Das Ministerium für Schule, Wissenschaft und Forschung des Landes Nordrhein-Westfalen erließ im Mai 2002 einen Runderlass - BASS 12 - 21 Nr. 15 - zur Übermittlung von Informationen und Auskünften an Eltern volljähriger Schülerinnen und Schüler. Dieser Erlass wurde beanstandet und seine Aufhebung verlangt.

Mit dem Eintritt der Volljährigkeit steht den betroffenen Schülerinnen und Schülern uneingeschränkt selbst das Grundrecht zu, über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen.

Der **Erlass verstößt** in zweifacher Hinsicht gegen dieses **Recht auf informationelle Selbstbestimmung**: Zum einen wird festgeschrieben, dass Angaben über die volljährigen Schülerinnen und Schüler bis zu ihrem schriftlichen Widerspruch an die Eltern übermittelt werden dürfen, da bis dahin das Einverständnis der Volljährigen unterstellt werden könne. Zum anderen ist bestimmt, dass die Schule die Eltern über den Widerspruch ihrer volljährigen Töchter und Söhne informiert. Für beide Datentransfers fehlt es an der erforderlichen Rechtsgrundlage: weder beruhen die jeweiligen Übermittlungen auf wirksamen Einwilligungen der Betroffenen, noch sind sie durch eine verfassungsgemäße Rechtsvorschrift gerechtfertigt.

Was zunächst die **Übermittlung von Informationen und Auskünften bis zum schriftlichen Widerspruch** der volljährigen Schülerinnen und Schüler anbetrifft, findet sich für diesen Datentransfer an die Eltern jedenfalls **keine Rechtsgrundlage** in § 3 Abs. 5 der Allgemeinen Schulordnung (ASchO): diese Vorschrift weist - datenschutzkonform - lediglich darauf hin, dass personenbezogene Angaben nur übermittelt werden dürfen, *soweit* das grundsätzliche *Einverständnis* der Volljährigen besteht. Der in Rede stehende Erlass, der als Auslegungsregel zu dieser Norm gedacht war, dient allerdings nicht ihrer Klarstellung, sondern **erweitert die Datenüber-**

mittlungsbefugnis. Er ersetzt die vorgesehene Einwilligungsregelung im Ergebnis durch eine Widerspruchslösung. Die Weitergabe von Informationen an die Eltern wäre hiernach faktisch nicht dann (ausnahmsweise) zulässig, wenn die Betroffenen wirksam eingewilligt hätten, sondern vielmehr nur dann (ausnahmsweise) unzulässig, wenn die Volljährigen der Übermittlung nicht - schriftlich! - widersprochen hätten; sie müssten mithin aktiv werden, um eine nicht gewollte Datenübermittlung zu verhindern. Das Widerspruchsrecht bleibt hinter dem Einwilligungserfordernis zurück und schränkt das informationelle Selbstbestimmungsrecht der Betroffenen unzulässig ein; der Erlass stellt keine hinreichende gesetzliche Grundlage für einen solchen Grundrechtseingriff dar.

Als Grundlage der Informationserteilung an die Eltern kommt derzeit ausschließlich die **Einwilligung** der Betroffenen in Betracht. Die Voraussetzung einer wirksamen Einwilligung sind in § 4 Abs. 1 DSG NRW normiert. Entgegen der Auffassung des Ministeriums ist der Runderlass insbesondere auch nicht mit § 4 Abs. 1 Satz 3 DSG NRW vereinbar, nach dem die Einwilligung der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere **Form** angemessen ist. Nach Maßgabe dieser Vorschrift ist nicht etwa die Erklärung des Willens, der Datenverarbeitung zuzustimmen, als solche entbehrlich, sondern vielmehr kann unter besonderen Umständen nur ein Abweichen von der regelmäßig erforderlichen Schriftform zugunsten einer **anderen Form der Erklärung** (beispielsweise mündlich, konkludentes Verhalten) angemessen sein. Aus bloßem Stillschweigen, dem kein eigener Erklärungswert zukommt, lässt sich daher auch in diesen Fällen keine wirksame Einwilligung fingieren.

Die zweite datenschutzwidrige Regelung, die der Runderlass enthält, betrifft die **Information der Eltern über den eingelegten Widerspruch**. Auch für die Übermittlung dieses personenbezogenen Datums fehlt es an der erforderlichen verfassungskonformen Rechtsgrundlage: Der Erlass vermag den Grundrechtseingriff nicht zu rechtfertigen, und die Volljährigen selbst haben mit ihrem Widerspruch explizit erklärt, dass sie mit der Übermittlung von Informationen an ihre Eltern gerade nicht einverstanden sind.

Vorsorglich wurde das Ministerium darauf hingewiesen, dass auch die Verabschiedung eines **dem Runderlass im Wortlaut entsprechenden formellen Gesetzes** datenschutzrechtlich bedenklich wäre. Abgesehen davon, dass wegen der bundesrechtlichen Volljährigkeitsregelung zunächst die Frage der Gesetzgebungskompetenz des Landes zu klären wäre, müsste die mit der Übermittlung verbundene Grundrechtsbeschränkung in materieller

Hinsicht jedenfalls nur dann hingenommen werden, wenn sie **verhältnismäßig**, also insbesondere zum Schutz öffentlicher Interessen unerlässlich wäre. Dabei ist im Hinblick auf das betroffene Rechtsgut eine strenge Prüfung der Verhältnismäßigkeit geboten, und zwar - anders als in dem genannten Runderlass geschehen - gesondert bezogen auf jeden konkreten Anlass, aus dem ein solcher Eingriff möglicherweise erlaubt werden soll. In Betracht gezogen werden können dabei überhaupt nur **besonders schwerwiegende Anlässe**. Eine pauschale Datenübermittlungsbefugnis oder gar -pflicht der Schulen wäre jedenfalls unverhältnismäßig und damit unzulässig. Geeignetheit und Erforderlichkeit der Benachrichtigung der Eltern müsste jeweils sorgfältig geprüft und festgestellt werden. Darzulegen wäre insbesondere auch, zu welchem verfassungslegitimen Zweck die Grundrechtseinschränkungen der Volljährigen erfolgen sollen; keine Rechtfertigung für diese Eingriffe dürfte sich aus dem in Art. 6 Abs. 2 Satz 1 Grundgesetz normierten **Elternrecht** herleiten lassen, das mit dem Eintritt der Volljährigkeit der Töchter und Söhne **erloschen** ist.

Da das Ministerium sich weigert, den rechtswidrigen Erlass aufzuheben, ist zu befürchten, dass die Schulleitungen nach diesem Erlass verfahren und dass damit landesweit in großem Umfang gegen den Datenschutz verstoßen wird.

Jede Datenweitergabe nach Maßgabe des Erlasses stellt einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht der oder des betroffenen Volljährigen dar. Schulen dürfen derzeit nur dann personenbezogene Angaben an die Eltern volljähriger Schülerinnen und Schüler übermitteln, wenn die Betroffenen zuvor wirksam in diesen Datentransfer eingewilligt haben.

11.4 Mangelhafte Personalaktenführung bei oberen Schulaufsichtsbehörden

Wer suchet, der findet sicherlich den einen oder anderen Mangel bei der gebotenen ordnungsgemäßen Führung einzelner Personalakten. Es war aber nicht damit zu rechnen, eine systematisch datenschutzwidrige Personalaktenführung im Schulbereich - mit Wissen und Billigung der Vorgesetzten - feststellen zu müssen.

Eine Lehrkraft konnte bei ihrer Akteneinsicht kaum noch nachvollziehen, welcher Stelle welche Personalaktendaten zu welchen Zwecken zugänglich

gemacht worden waren. Eine Überprüfung ergab, dass die einzelnen Blätter der Akte nicht ordnungsgemäß nummeriert waren und das Inhaltsverzeichnis, das Aktenausgabeblatt sowie das Schlussblatt gar nicht oder nicht richtig geführt wurden. Die Lehrkraft konnte also nicht erkennen, was Gegenstand ihrer Akte war und wer was über sie erfahren hatte. Die erforderliche **Transparenz** im Umgang mit Personalaktendaten war somit **nicht gegeben**.

Insbesondere entsprach die Aufbewahrung von **Gesundheitsdaten** aus ärztlichen Begutachtungen in keiner Weise den Anforderungen an einen erhöhten Schutz sensibler personenbezogener Daten, wie sie in Nr. 3.3 der Verwaltungsvorschriften zu § 102 Landesbeamtengesetz (LBG) verbindlich vorgegeben sind:

- Aufbewahrung in einem verschlossenen Umschlag und
- besonderer Vermerk jeder Einsichtnahme in die ärztlichen Unterlagen.

Hinzu kam, dass das amtsärztliche Gutachten zu einer beantragten Pflichtstundenermäßigung - entgegen den Regelungen des § 24 Abs. 2 Gesundheitsdatenschutzgesetz Nordrhein-Westfalen (GDSG NW) - eine **Diagnose** enthielt, ohne dass die Erforderlichkeit dieser Angabe für die zu treffende Entscheidung ersichtlich wäre.

Hier ging es nicht lediglich um ein Versehen im Einzelfall. Es stellte sich vielmehr heraus, dass bei der betreffenden Bezirksregierung in der Regel **alle Personalakten** der Schulabteilung aus Gründen der Verwaltungsvereinfachung **ohne Beachtung der gesetzlichen Vorgaben** und der Richtlinien zur ordnungsgemäßen Führung von Personalakten geführt werden. Die damit verbundene gravierende Beeinträchtigung der betroffener Lehrkräfte in ihrem Anspruch auf Schutz ihrer Daten vor unbefugter Offenbarung sowie auf Einsicht in ihre vollständige Personalakte (§ 102c Absatz 1 LBG) ist den Vorgesetzten bekannt und wird von diesen unter Hinweis auf den Personalmangel in Kauf genommen. Den Empfehlungen zur künftigen Aktenführung will die Schulabteilung daher nur zum Teil entsprechen. Folgende **Mängel** sind **weiterhin zu beanstanden**:

- Amtsärztliche Gutachten können weiterhin grundsätzlich Diagnosedaten enthalten;
- Inhaltsverzeichnis und Schlussblatt werden nicht kontinuierlich oder gar nicht geführt;

- bei Versendung von Personalakten an Stellen außerhalb der Schulaufsichtsbehörde erhalten nur die Gerichte vollständig paginierte Akten oder Aktenteile unter Angabe der genauen Blattzahlen. Bei den übrigen Versendungen (etwa an das Gesundheitsamt) ist grundsätzlich für die Betroffenen nicht nachvollziehbar, welche Personalaktendaten zugänglich gemacht worden sind.

Im Hinblick auf die vermutlich landesweite Problematik ist das Schulministerium darauf aufmerksam gemacht worden, um Aufsichtsmaßnahmen zu ergreifen. Eine Äußerung des Ministeriums dazu ist nach mehr als einem Jahr trotz mehrfacher Erinnerungen nicht eingegangen.

Gesetzliche Vorgaben und Verwaltungsvorschriften zum Schutz von Daten der Lehrkräfte sind zwingend einzuhalten. Die rechtswidrige Verfahrensweise der Bezirksregierung ist beanstandet worden.

11.5 Genealogische und zeitgeschichtliche Forschung

Aller Zukunftsorientierung unserer schnelllebigen Zeit zum Trotz ist die Beschäftigung mit der Vergangenheit nicht unmodern geworden, wie viele Anfragen zu genealogischer oder zeitgeschichtlicher Forschung zeigen. Dabei werden häufig Daten verstorbener und/oder noch lebender Personen verarbeitet.

„Zurück zu den Wurzeln", denkt sich Frau X und möchte endlich in Erfahrung bringen, wer ihre Vorfahren und deren Abkömmlinge waren - doch im Standesamt, das sie zu diesem Zweck aufsucht, wird ihr zu möglichen Datenquellen der Zugang verwehrt. Familie Y ist da schon weiter und plant, das Ergebnis ihrer umfangreichen Ahnenrecherche ins Internet zu stellen - müssen dafür wirklich alle Lebenden einwilligen, und was ist mit den Daten der Verstorbenen? Rentner Z will sich seinen langgehegten Traum erfüllen und im Bereich Geschichte promovieren; er begehrt Einsicht in historische Akten, die sich im Staatsarchiv befinden.

Was die **Erhebung** von Daten aus **besonderen Quellen** betrifft, finden gegebenenfalls bereichsspezifische Spezialvorschriften Anwendung, so auch im Fall der Frau X. Will sie im Standesamt die **Personenstandsbücher** ihres Großvaters einsehen, wird ihr, sofern sie ihre Abstammung in gerader Linie nachweisen kann, die Einsichtnahme gestattet werden; möchte sie dagegen Personenstandsbücher ihrer Großtante einsehen, wird sie in der

Regel mit diesem Begehren scheitern, wenn sie nicht die Vollmacht einer oder eines Berechtigten aus der entsprechenden Seitenlinie vorlegen kann. Was zunächst widersprüchlich erscheint, findet gleichwohl eine gesetzliche Grundlage in den unterschiedlichen Vorschriften des **Personenstandsgesetzes** (hier: § 61 Abs. 1 Satz 1 und Satz 3 PStG). Die Nutzung **öffentlichen Archivguts** in Nordrhein-Westfalen durch Dritte ist dagegen in § 7 **Archivgesetz** (ArchivG NW) differenziert geregelt. Nach Ablauf der im einzelnen bestimmten Sperrfristen kann das Archivgut nutzen, wer ein berechtigtes Interesse an der Nutzung glaubhaft macht, zum Beispiel die Nutzung zu wissenschaftlichen Zwecken begehrt. Gelingt es Herrn Z. sein wissenschaftliches Interesse glaubhaft zu machen, dürften der Nutzung des Archivguts nach Maßgabe dieser Vorschrift grundsätzlich keine Hindernisse entgegenstehen; allerdings kann sie an Bedingungen und Auflagen gebunden werden.

Ob und inwieweit es im Übrigen aus datenschutzrechtlicher Sicht zulässig ist, Daten Dritter zu **verarbeiten**, insbesondere auch zu **veröffentlichen**, hängt - wie Familie Y zutreffend erkannt hat - in der Regel zunächst davon ab, ob diese dritten Personen noch leben oder bereits verstorben sind. Datenschutzrechtliche Vorschriften schützen die Einzelperson davor, dass ihre **personenbezogenen Daten**, also alle Einzelangaben über persönliche und sachliche Verhältnisse dieser **natürlichen Person** (vgl. § 3 Abs. 1 DSG NRW; § 3 Abs. 1 BDSG), in unzulässiger Weise verarbeitet werden. „Natürliche" sind alle lebenden Personen; Daten **Verstorbener** werden dagegen vom Schutzbereich der datenschutzrechtlichen Vorschriften grundsätzlich nicht umfasst. Ausnahmen, in denen auch die Daten von Verstorbenen in besonderer Weise geschützt werden, finden sich in einzelnen Spezialvorschriften; ein besonderes Schutzbedürfnis kann sich aus der Quelle (beispielsweise Archiv) oder der Art der Daten (etwa Gesundheits- oder Sozialdaten) ergeben. Auch ist zu bedenken, dass das Ansehen der Verstorbenen nicht durch beispielsweise ehrverletzende Äußerungen beeinträchtigt werden darf. Ist keiner dieser Ausnahmetatbestände gegeben, erheben sich gegen die Verarbeitung der Daten von Verstorbenen keine datenschutzrechtlichen Bedenken. Deshalb darf Familie Y jedenfalls die Hauptlebensdaten der verstorbenen Familienmitglieder (etwa Namen, Geburts-, Eheschließungs- und Sterbedaten), die sie aus Zeitungsanzeigen, Grabinschriften, Veröffentlichungen in Amtsblättern, Stadtanzeigern, Gemeindebriefen und vergleichbaren Quellen erhoben hat, veröffentlichen und als Ergebnis ihrer genealogischen Forschung ins Internet stellen.

Wollen die Angehörigen der Familie Y als Privatpersonen Daten ihrer **lebenden** Verwandten im Internet **veröffentlichen**, so ist dies nach Maßgabe des § 4 Abs. 1 BDSG nur zulässig, soweit es eine Rechtsvorschrift erlaubt oder die betroffenen Personen eingewilligt haben. Zwar heißt es in §§ 1 Abs. 2 Nr. 3, 27 Abs. 1 Satz 2 BDSG, das BDSG finde keine Anwendung, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolge. Selbst wenn die genealogische Forschung jedoch ursprünglich zu rein familiären Zwecken betrieben worden ist, wird diese Zweckbindung jedenfalls durch die Veröffentlichung der Daten im **Internet** überschritten. Mittels dieses Mediums werden die Daten nämlich weltweit einem unbeschränkten Personenkreis zugänglich gemacht, so dass keine ausschließlich private, familiäre Nutzung vorliegt. Die Regelungen des BDSG finden deshalb Anwendung. Nach Maßgabe des § 28 Abs. 1 Satz 1 Nr. 3 BDSG darf Familie Y die personenbezogenen Daten Dritter im Internet nur veröffentlichen, wenn die Daten **allgemein zugänglich** sind. Überwiegt allerdings offensichtlich ein schutzwürdiges Interesse daran, dass eine Veröffentlichung unterbleibt, so ist dem Rechnung zu tragen. Stammen die Angaben über die Lebenden nicht aus für die Öffentlichkeit allgemein und frei zugänglichen Quellen, ist eine Veröffentlichung der Daten nur mit **Einwilligung** der Betroffenen zulässig. Die Voraussetzungen einer wirksamen Einwilligung sind in § 4a BDSG normiert.

Herr Z hat bei der Auswertung seines historischen Datenmaterials und bei der Veröffentlichung des Ergebnisses seiner zeitgeschichtlichen Forschung insbesondere die **Bedingungen und Auflagen** zu erfüllen, die das **Archiv** für die Nutzung des Archivguts - in der Regel gerade auch zum Schutz verstorbener und/oder lebender Personen, auf das sich die historischen Unterlagen beziehen - festgesetzt hat. Verarbeitet er in seiner Dissertation Daten von Lebenden, hat er darüber hinaus den allgemeinen datenschutzrechtlichen Anforderungen Rechnung zu tragen.

11.6 Forschung mit Blut- und Gewebeproben

Im Zeitalter der Gentechnik haben viele Forschungsprojekte im Gesundheitsbereich die Untersuchung von Blut- und Gewebeproben zum Gegenstand. Es fragt sich, ob und inwieweit sich die allgemeinen Datenschutzgrundsätze auf diese Vorhaben übertragen lassen.

Aus Gründen des Datenschutzes sollen Daten zu wissenschaftlichen Zwecken möglichst in **anonymisierter** Form verarbeitet werden, also ohne Personenbezug oder -beziehbarkeit. Stehen einer Anonymisierung wissenschaftliche Gründe entgegen, sind die personenbezogenen Daten zu **pseudonymisieren**, dass heißt so zu verändern, dass die Einzelangaben ohne Nutzung einer Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßig hohen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Nur wenn weder eine Anonymisierung noch eine Pseudonymisierung möglich ist, dürfen Daten zu Forschungszwecken - unter bestimmten weiteren Voraussetzungen - **personenbezogen oder -beziehbar** verarbeitet werden. Der Personenbezug ist aber dann zum frühest möglichen Zeitpunkt zu löschen.

Dieses Abstufungsmodell gilt prinzipiell für jedes Forschungsvorhaben, also auch dann, wenn im Rahmen eines Projekts Blut- und Gewebeproben entnommen, analysiert und aufbewahrt werden sollen. Im Hinblick auf die Besonderheit dieses Untersuchungsgegenstandes fragt sich indes, ob sich die Personenbeziehbarkeit dieser Datensätze tatsächlich überhaupt ausschließen lässt. Zwar können die Proben - ähnlich wie Fragebogen - entweder von vornherein ohne Namen und sonstige äußere Hinweise auf die betroffenen Personen untersucht oder aber mit einer Nummer versehen werden, die sich nur über eine besondere Liste einer konkreten Person zuordnen lässt; doch die Datensätze deshalb als anonym oder pseudonym anzusehen, erscheint zumindest bedenklich.

Der **genetische Code** ist diesen Proben nämlich weiterhin immanent und im Übrigen reproduzierbar. Er ist nicht nur personenbezogen, sondern vielmehr sogar **personengebunden**: in ihm sind alle genetischen Informationen einer bestimmten Person enthalten, die diese bis ins letzte erblich bedingte Detail beschreiben. Ebenso wie ein Foto nur eine andere Darstellungsform einer bestimmten Person ist - nämlich deren zweidimensionale visuelle Abbildung auf Fotopapier unter Nutzung fototechnischer Mittel - ist auch der genetische Code das vollständige Abbild einer einmaligen Person: Ihre besondere Darstellung in codierter Form. Ein - vermeintliches - Pseudonym lässt sich sowohl durch den Vergleich zweier vorhandener Proben als auch aufgrund des genetischen Fingerabdrucks selbst durchbrechen. Es ist vorstellbar, dass es zukünftig möglich sein wird, mit Methoden der Bioinformatik aus der Gesamtheit der genetischen Informationen, die der Gencode enthält, beispielsweise eine visuelle Darstellung der betroffenen Person abzuleiten; dies ist bereits heute schon (eingeschränkt) möglich

durch entsprechende algorithmische Auswertungen von Informationen, wie sie beispielsweise Kernspintomographen liefern. Mithin ist nicht auszuschließen, dass die Datensätze künftig auch ohne Nutzung einer - äußeren - Zuordnungsfunktion einer bestimmten Person zugeordnet werden können.

Was ist zu tun? Was die äußeren personenbezogenen Merkmale betrifft, mit denen Blut- und Gewebeproben im Rahmen des Forschungsvorhabens versehen werden, gelten keine Besonderheiten: Namensangaben sowie Codierungen und Zuordnungslisten sind, sobald es der Forschungszweck zulässt, von Proben **zu trennen** und **zu löschen**. Dem noch verbliebenen „Restrisiko", die Proben möglicherweise mittels der in ihnen selbst enthaltenen Daten auf bestimmte Personen beziehen zu können, kann derzeit nur dadurch Rechnung getragen werden, dass zum einen Forschungs- und **Verwendungszweck** sowie **Speicherdauer** der Proben restriktiv festgelegt werden, und zum anderen die Teilnehmenden an dem Vorhaben in Bezug auf die Verwendung und Aufbewahrung der Proben besonders eingehend aufgeklärt werden und auf der Grundlage dieser umfassenden Aufklärung in die Teilnahme einwilligen. Im Umfang der informierten Einwilligungen, also insbesondere nur zu dem benannten Zweck, auf die beschriebene Weise und für die festgelegte Dauer, dürfen die Proben zu Forschungszwecken verarbeitet werden. Danach sind sie unverzüglich zu vernichten.

Wegen der besonderen datenschutzrechtlichen Risiken der Forschung mit Gen- und Blutproben bedarf es einer besonders detaillierten Aufklärung der teilnehmenden Personen. Die Forscherinnen und Forscher sind eng an den Zweckbindungsgrundsatz und die beschränkte Speicherdauer der Proben gebunden. Jegliche Erweiterung des ursprünglichen Forschungsvorhabens bedarf neuer Einwilligungen der betroffenen Personen.

12 Kommunales

Der Bundesgesetzgeber hat das **Melderechtsrahmengesetz** (MRRG) mit Gesetz vom 25. März 2002 novelliert. Insbesondere wurde mit dem MRRG die Grundlage für einen **elektronischen Datenaustausch** zwischen dem Einwohnermeldeamt einerseits und Bürgerinnen und Bürgern oder sonstigen Behörden andererseits geschaffen. **Einfache Melderegisterauskünfte** beispielsweise, die schon nach der bisherigen Rechtslage jeder Person zur Ermittlung des Vor- und Nachnamens, eines eventuellen Doktorgrades und der Anschrift einer dritten Person zu beantworten sind, können nach der Umsetzung der Novelle in das Meldegesetz des Landes Nordrhein-Westfalen mit Hilfe des Internet elektronisch abgerufen werden. War schon die bisherige Rechtslage aus datenschutzrechtlicher Sicht unbefriedigend, weil die Einzelperson die amtliche Übermittlung dieser Daten nur im Falle des Vorliegens einer erheblichen Gefahr für Leben, Gesundheit, Freiheit oder ähnlicher schutzwürdiger Belange ihrer eigenen oder einer anderen Person durch Einrichtung einer Auskunftssperre verhindern konnte, so wird diese Situation durch die bevorstehende Einführung einer **Online-Abrufmöglichkeit** weiter verschärft, weil die Nachfrage danach vom heimischen PC erfolgen kann. Hier konnte im Laufe des Gesetzgebungsverfahrens von den Datenschutzbeauftragten des Bundes und der Länder erreicht werden, dass eine Einzelperson den elektronischen Zugriff auf ihre Daten jedenfalls durch einen **Widerspruch** verhindern kann, ohne dass es dazu besonderer Umstände wie nach der bisherigen Rechtslage bedürfte. Ist ein Widerspruch nicht erfolgt, so ist die elektronische Melderegisterauskunft jedenfalls auch dadurch erschwert, dass zu der betroffenen Person neben Vor- und Familiennamen zwei weitere im Melderegister gespeicherte Daten zu deren Identifizierung zutreffend angegeben werden müssen. Weiterhin verbietet eine eingetragene Auskunftssperre nach dem MRRG gegenüber der früheren Rechtslage die Erteilung von Auskünften nicht mehr generell, sondern löst lediglich die Verpflichtung der Meldebehörde aus, die betroffene Person vor der Erteilung einer Auskunft zu hören und ihre Interessen zu berücksichtigen. Damit stellt eine einmal eingetragene Auskunftssperre kein unüberwindbares Hindernis für die Erteilung von Auskünften mehr dar, sondern es wird lediglich sichergestellt, dass Auskünfte nur nach Anhörung der betroffenen Person und nach gründlicher Prüfung des Einzelfalles unter Abwägung der Interessen der antragstellenden und der betroffenen Person erteilt werden.

Insoweit wurde der Hinweis gegeben, dass die Betroffenen bei Beantragung einer **Auskunftssperre** der Meldebehörde bereits hoch sensible Einzelheiten, die ihre Gefährdungssituation begründen, zu offenbaren haben. Sie müssen sich daher darauf verlassen können, dass durch eine Auskunftssperre verhindert wird, dass Personen, von denen eine Bedrohung ausgeht, entweder durch einen direkten Zugriff auf die Daten oder auf Umwegen - beispielsweise durch vorgetäuschte rechtliche Interessen - die Auskunft erhalten. Außerdem soll diese Auskunftssperre nunmehr automatisch nach Ablauf des zweiten auf die Beantragung folgenden Kalenderjahres enden, wobei das Risiko einer nicht rechtzeitigen Verlängerung durch die betroffene Person besteht. Demgegenüber hatte die Behörde nach der früheren Rechtslage selbst zu überprüfen, ob die unbefristete Sperre gegebenenfalls aufzuheben war.

Ungeachtet erheblicher datenschutzrechtlicher Bedenken gegen eine weiter ausufernde Datenübermittlung wurde ebenfalls ein **Auskunftsrecht der Vermieterinnen und Vermieter** über Personen etabliert, die in einer ihnen gehörenden Wohnung leben.

Im Zuge der Diskussion nach dem 11. September 2001 erfuhr das Passgesetz ebenso wie das Personalausweisgesetz eine Erweiterung, die die Aufnahme weiterer **biometrischer Merkmale** (siehe unter 3.2) **in Ausweisdokumente** ermöglicht. Neben den bereits bisher in den Ausweisdokumenten vorhandenen Merkmalen (Lichtbild und Unterschrift) dürfen künftig auch solche der Finger, Hände oder des Gesichts in verschlüsselter Form in den Ausweispapieren gespeichert werden. Eine bundesweite **Referenzdatei** darf **nicht eingerichtet** werden. Weiterhin ist geregelt, dass die biometrischen Merkmale nur verwendet werden dürfen, um die Echtheit des Dokumentes und die Identität der Inhaberin oder des Inhabers zu prüfen. Neben der Frage, ob die Einführung biometrischer Merkmale zur Bekämpfung des internationalen Terrorismus überhaupt geeignet ist (insbesondere weil nicht einmal alle Staaten des Schengener Abkommens diese einführen wollen), sind angesichts der bereits heute bestehenden fast hundertprozentigen Fälschungssicherheit der deutschen Ausweispapiere damit auch **Zweifel an der Erforderlichkeit** dieser Maßnahmen begründet.

Ihre Umsetzung, besonders die sonstige Verarbeitung und Nutzung der biometrischen Merkmale, bleibt einem noch zu erlassenden Bundesgesetz vorbehalten. Damit ist das Ausmaß, in dem das Grundrecht auf informationelle Selbstbestimmung durch die Aufnahme weiterer

biometrischer Merkmale in Ausweispapiere betroffen ist, noch unklar. Das Grundrecht schützt die für eine Demokratie wesentliche Handlungs- und Entscheidungsfreiheit der Bürgerinnen und Bürger vor staatlicher Kontrolle, indem der Speicherung und Nutzung persönlicher Daten Grenzen gesetzt werden. Eine Nutzung der biometrischen Merkmale zu anderen als **Identifizierungszwecken**, etwa zum Abgleich mit Dateien des Verfassungsschutzes, zur Auswertung von Videoaufzeichnungen von Demonstrationen wie auch zu privatrechtlichen Zwecken (Versicherungen, Gesundheitssystem) muss daher ausgeschlossen sein. Abzulehnen sind außerdem Kontrollen, die ohne Mitwirkung der davon Betroffenen möglich und diesen unter Umständen nicht einmal bewusst sind (so genannte **passive Systeme**). Darüber hinaus muss sichergestellt sein, dass keine überschießenden Daten (zum Beispiel zur Erkennung gesundheitlicher Zustände, Stress oder Müdigkeit) erhoben und verarbeitet werden. Problematisch ist weiter, dass auch bei ständigem technischen Fortschritt eine wirklich fehlerfreie Identifikation anhand biometrischer Merkmale nicht möglich ist. Kommt es in Einzelfällen (etwa bei Zugangskontrollen) zu Zurückweisungen Berechtigter, muss eine die Betroffenen nicht diskriminierende Aufklärung gewährleistet sein (vgl. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002, Abdruck im Anhang, Nr. 13).

12.1 Bekanntgabe personenbezogener Daten in der Kommunalverwaltung

Immer wieder werden Fragen gestellt, die die Bekanntgabe personenbezogener Daten in Rats- und Ausschusssitzungen (etwa auch in Sitzungsvorlagen) betreffen.

Personenbezogene Daten dürfen offenbart werden, soweit nicht schützenswerte Interessen Einzelner oder Belange des öffentlichen Wohls überwiegen. Dabei ist eine Abwägung zwischen dem Anspruch der betroffenen Person auf Schutz ihrer Daten und dem Prinzip der Öffentlichkeit von Rats- und Ausschusssitzungen vorzunehmen. Darüber hinaus ist stets der verfassungsrechtliche **Grundsatz der Verhältnismäßigkeit** zu beachten, wobei an die Erforderlichkeit der Bekanntgabe personenbezogener Daten ein strenger Maßstab zu stellen ist. Zu prüfen ist also in jedem konkreten **Einzelfall**, ob den Rats- und Ausschussmitgliedern auch ohne Offenbarung der personenbezogenen

Daten eine ausreichende Grundlage für eine sachgerechte Entscheidung zur Verfügung steht. Nur wenn die Bekanntgabe der Daten zur Aufgabenerfüllung unbedingt notwendig ist, ist sie zulässig. Erforderlichenfalls ist dann aber die Öffentlichkeit von der Sitzung auszuschließen; die Sitzungsteilnehmenden sind zur Verschwiegenheit verpflichtet. Ist eine Bekanntgabe dagegen lediglich dienlich, kommt allenfalls der Weg über eine Einwilligung der betroffenen Bürgerinnen und Bürger in Betracht. Nach den dargelegten Grundsätzen ist beispielsweise eine Bekanntgabe personenbezogener Daten für die Beschlussfassung von Bebauungsplänen in aller Regel nicht notwendig und damit unzulässig, weil hier die Angabe sachbezogener Daten für eine fehlerfreie Ausübung des Planungsermessens grundsätzlich genügt.

Andererseits beklagten Rats- und Ausschussmitglieder, nicht in ausreichendem Umfang von der Kommunalverwaltung Informationen zu erhalten. Auch insoweit gilt:

Rats- und Ausschussmitgliedern dürfen diejenigen Daten zur Verfügung gestellt werden, die für die Aufgabenerfüllung des Rates und der Ausschüsse erforderlich sind. Die Kontrolle der Verwaltung durch den Rat muss dabei gewährleistet bleiben.

12.2 Meldebescheinigung auch für einen einzigen Zweck

Müssen Meldebescheinigungen immer den vollständigen Meldedatensatz enthalten?

In Meldebescheinigungen ist häufig eine Vielzahl von Daten (zum Beispiel der Familienstand) enthalten, deren Inhalte den benötigten Zweck (Ummeldung eines Kraftfahrzeuges) weit überschreiten. Das Meldegesetz des Landes Nordrhein-Westfalen hat zu Form und **Inhalten von Meldebescheinigungen**, die von Bürgerinnen und Bürgern häufig zum Nachweis eigener Daten bei anderen Behörden benötigt werden, keine Regelungen getroffen. Da vielfach gegenüber dem Meldeamt keine Angaben zum Zweck der benötigten Bescheinigung gemacht werden, wird diese häufig mit einer pauschalen Zusammenstellung von Daten ausgestellt.

Zur Vermeidung von Verstößen gegen den Grundsatz der Datensparsamkeit wurde in einem konkreten Fall empfohlen, bei Beantragung einer Meldebescheinigung die Bürgerinnen und Bürger umfassend zu den Einschränkungsmöglichkeiten zu beraten und den Verwendungszweck zu

erfragen, um die Meldebescheinigungen auf den dementsprechend benötigten Dateninhalt zu beschränken. Dem ist die Stadt erfreulicherweise gefolgt.

12.3 Datenübermittlung für die Kindergartenbedarfsplanung

Eine Gemeinde bat um Beantwortung der Frage, ob dem Kreisjugendamt zum Zweck der Bedarfsplanung Daten aus dem Melderegister übermittelt werden dürfen.

Im Einzelnen war folgendes beabsichtigt: Die Meldebehörde übermittelt einmal jährlich eine Liste sämtlicher Kinder, die mit Beginn oder im Laufe des Kindergartenjahres das dritte Lebensjahr vollenden, mit vollem Namen, Geburtstag und Anschrift an die Kreisjugendämter. Diese Liste wird einmal monatlich durch Übermittlung der Zu- und Wegzugsdaten aktualisiert. Bei dem Kreisjugendamt erfolgt dann ein **Abgleich** mit den bei den Gemeinden vorhandenen Übersichten über die in den Einrichtungen aufgenommenen Kinder. Ziel war, hierdurch eine **bedarfsgerechte Planung** zu erreichen, weil Doppelanmeldungen sowie Nichtabmeldungen bereinigt werden können. Es stellte sich außerdem die Frage, ob eine Datenübermittlung von den Kindertagesstätten selbst an die Kreise zulässig sei. Den Jugendämtern als örtlichen Trägern der öffentlichen Jugendhilfe obliegt nach § 10 des Gesetzes über Tageseinrichtungen für Kinder die Planungsverantwortung für Kindergärten.

§ 31 Abs. 5 des Meldegesetzes Nordrhein-Westfalen lässt die vorgesehene Datenübermittlung aus dem Melderegister an das Kreisjugendamt unter der Voraussetzung zu, dass die Übermittlung nicht allein durch eine einzelne, sondern durch alle Meldebehörden des mit der Bedarfsplanung betrauten Kreises gleichartig erfolgt. Die Datenübermittlung an die Kreise ist daher unter der vorstehenden Maßgabe zulässig. Eine Datenübermittlung von den Kindertagesstätten selbst an die Kreise muss jedoch unterbleiben, weil eine Rechtsgrundlage hierfür nicht besteht.

12.4 Datenschutzgerechte Ausgestaltung von Bürgerbüros

Kommunen bitten immer wieder um Hilfestellung bei der datenschutzgerechten Ausgestaltung ihrer Bürgerbüros. Die insoweit aufgeworfenen Fragen lassen sich oft durch die zur Verfügung stehenden Orientierungshilfen beantworten.

Zunächst ist auf die Anforderungen des Datenschutzes im Bereich der automatisierten Datenverarbeitung zu achten. Im Übrigen muss insbesondere darauf Wert gelegt werden, dass die **Datensicherheit** auch in **akustischer** und **visueller Hinsicht** gewährleistet wird. Da Bürgerbüros oft räumlich beengt in Großraumbüros untergebracht sind, wird dies häufig nur durch den Einsatz spezieller schallschluckender Raumtrennsysteme sicher zu stellen sein. Sofern in den vorgetragenen Fällen keine besonderen Problemkonstellationen vorlagen, wurden die anfragenden Stellen regelmäßig auf die Ausführungen im 14. Datenschutzbericht 1999 (unter 5.1.5.1.2; S. 88, 90) verwiesen.

Weitere Empfehlungen für eine serviceorientierte Verwaltung enthält die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder veröffentlichte umfassende Informationsbroschüre „Vom Bürgerbüro zum Internet" (abrufbar unter: www.lfd.nrw.de).

13 Soziales

Kann die von einer hilfesuchenden Person beantragte Sozialleistung von einem Sozialleistungsträger nach den anzuwendenden rechtlichen Vorschriften nicht gewährt werden, widerspricht dies in manchen Fällen dem subjektiven Gerechtigkeitsempfinden. Um die Entscheidung selbst nachvollziehen oder prüfen zu können, ob die Behörde beispielsweise alle maßgeblichen Umstände berücksichtigt hat, steht den Beteiligten nach § 25 des Zehnten Buches des Sozialgesetzbuches - Verwaltungsverfahren - (SGB X) ein **Akteneinsichtsrecht** in die das Verfahren betreffenden Akten zu, „soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist". Mit dieser Vorschrift hat der Gesetzgeber für den Bereich der Sozialdaten dem Prinzip der grundsätzlichen Aktenöffnung für die Beteiligten eines Verfahrens Rechnung getragen. Allerdings ist die Behörde zur Gestattung der Akteneinsicht nicht verpflichtet, soweit berechtigte Interessen der an dem Verfahren Beteiligten oder dritter Personen entgegenstehen.

Unabhängig hiervon ist Betroffenen nach § 83 SGB X auf Antrag **Auskunft** zu erteilen über die zu ihrer Person gespeicherten Sozialdaten, außer für den Fall, dass die Daten wegen der überwiegenden berechtigten Interessen dritter Personen geheim gehalten werden müssen. Die Auskunft kann auch in Form der Akteneinsicht erfolgen.

Der Anspruch auf ein Akteneinsichtsrecht für den Bereich der Sozialdaten richtet sich allein nach den speziellen Vorschriften des Sozialgesetzbuchs. Kommt die Behörde nach Überprüfung zu dem Ergebnis, dass eine Akteneinsicht nicht zu gestatten ist, haben Hilfesuchende auch nicht über andere Vorschriften ein Recht auf Akteneinsicht.

Dies gilt insbesondere für das Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (**Informationsfreiheitsgesetz Nordrhein-Westfalen - IFG NRW**) vom 27. November 2001. Dieses sieht zwar vor, dass jede natürliche Person gegenüber den in diesem Gesetz genannten öffentlichen Stellen einen Anspruch auf Zugang zu den bei der Stelle vorhandenen amtlichen Informationen hat. Soweit aber besondere Rechtsvorschriften über den Zugang zu personenbezogenen Sozialdaten bestehen, gehen diese speziellen Vorschriften denen des IFG NRW vor.

Wie bereits im 15. Datenschutzbericht 2001 unter 10., S. 99, ausgeführt, erfordern verschiedene Aufgabenstellungen der Sozialleistungsträger, dass für die Bearbeitung und Entscheidung über das Anliegen der Betroffenen Daten erhoben und verarbeitet werden müssen. Über die **Rechtmäßigkeitsvoraussetzungen** für diese Datenverarbeitung werden die Betroffenen nicht selten **unzureichend informiert**.

Es kommt immer noch vor, dass Sozialämter Hilfesuchenden die Erhebung und Verarbeitung ihrer Daten in der Weise begründen, dass sie eine Vorschrift anführen, die der Behörde lediglich eine bestimmte Aufgabe zuweist (**Aufgabenzuweisungsnorm**). Soweit jedoch eine zusätzliche Vorschrift nicht ausdrücklich eine Datenerhebung und -verarbeitung vorsieht oder zulässt (**Befugnisnorm**), ist eine allein auf eine Aufgabenzuweisungsnorm gestützte Datenerhebung und -verarbeitung unzulässig. Auch ein Hinweis auf eine etwaige Mitwirkungspflicht der Antragstellenden ist für sich allein keine Ermächtigungsgrundlage für eine Datenerhebung und -verarbeitung.

Voraussetzung für die Zulässigkeit einer Datenerhebung ist immer, dass die einzelnen Daten für die Aufgabenerfüllung der erhebenden Stelle erforderlich sein müssen. **Erforderlich** bedeutet, dass die Angaben für die Aufgabenerledigung des Leistungsträgers unbedingt notwendig sind. Wenn solche Daten lediglich dienlich oder nützlich sind, so fehlt es an der vom Gesetz verlangten Erforderlichkeit.

Die nach einer Erhebung vorgesehene weitere Verarbeitung und Nutzung der (Sozial-)Daten ist nur zulässig, soweit es eine Rechtsvorschrift ausdrücklich erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat. Allerdings kann eine Einwilligung nur für den Einzelfall eingeholt werden, nicht jedoch als generelle Verfahrensweise, da andernfalls die Intention des Gesetzgebers über die Zulässigkeit der Datenverarbeitung umgangen würde.

Im Übrigen hat der Bundesgesetzgeber im Berichtszeitraum durch verbesserte oder neue **Unterrichtungsverpflichtungen** der Leistungsträger gegenüber den Betroffenen (§ 67a Abs. 3 und Abs. 5 SGB X) die **Transparenz** der Verarbeitung von Sozialdaten für die Betroffenen deutlich **erhöht**.

13.1 Neue Formulare im Sozialbereich

Nach der Kritik im 15. Datenschutzbericht 2001 unter 10.1, S. 99-101, an teils völlig veralteten Formularen und Vordrucken im Bereich der Sozialämter ist es in dem zurückliegenden Berichtszeitraum nunmehr gelungen, in verschiedenen Verwaltungsbereichen, bei denen die personenbezogenen Daten dem Sozialgeheimnis unterliegen, für eine Überarbeitung der zum Teil bis in die 60er Jahre zurückreichenden Formulare für die Erhebung von Sozialdaten zu sorgen.

Im Zusammenwirken mit den verschiedenen betroffenen Stellen, einer Vordruckkommission und den jeweiligen Aufsichtsbehörden wurde ein Anfang gemacht, dem Recht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger auch bereits bei der **Datenerhebung mittels Formular** oder Vordruck Rechnung zu tragen. Dabei ist andererseits mehr als deutlich geworden, dass es für die Sozialverwaltung nicht einfach ist, sich von traditionellen Praktiken der Datenerhebung zu verabschieden. Gleichzeitig fehlt vielfach das Bewusstsein, dass zwischen dem Recht auf informationelle Selbstbestimmung der Antragstellenden, ihrer Angehörigen, im Haushalt lebenden Dritten und sonstigen Dritten zu unterscheiden ist. Auch die Tatsache, dass Kinder, je nach Einsichtsfähigkeit etwa ab dem 14. Lebensjahr, ihr Recht auf informationelle Selbstbestimmung selbst geltend machen können, scheint wenig bekannt zu sein.

Auch wenn die Bemühungen in dieser Hinsicht bisher nur vereinzelt zu Ergebnissen geführt haben, bleibt die konkrete Hoffnung, dass die Datenerhebung in verschiedenen Verwaltungsbereichen bald auf **datenschutzkonform** neu gestaltete und überarbeitete Formulare sowie Vordrucke umgestellt wird. Dies gilt insbesondere für die Versorgungsverwaltung, einzelne Sozialämter und einen Leistungsträger aus dem Bereich der gesetzlichen Krankenversicherung.

Zusätzlich ist erreicht worden, dass eine Reihe von Formularen nicht mehr verwendet werden oder die Verwaltungspraxis entsprechend der bestehenden Rechtslage abgeändert und angepasst wurde.

Im Hinblick auf die sehr große Zahl von Formularen und Vordrucken, die bei den verschiedenen Leistungsträgern im Sozialbereich in Anwendung sind, wird deutlich, dass bisher nur ein erster Anfang gemacht werden konnte, allerdings ein Anfang, der insgesamt die Hoffnung auf eine grundlegende Änderung der Haltung der Sozialleistungsträger gegenüber den Erfordernissen des Datenschutzes vermittelt.

13.2 Umorganisation der Versorgungsverwaltung - Nachholbedarf beim Datenschutz

Das Sozialministerium hat die Versorgungsverwaltung grundlegend umstrukturiert. Unter dem Aspekt „Optimierung von Bürgerservice und Kundenorientierung" sind verschiedene Projekte und Verfahren implementiert worden, die auch datenschutzrechtlich relevant sind. Auf Vorschlag des Ministeriums wurde eine Arbeitsgruppe mit der Zielsetzung eingerichtet, sämtliche in der Versorgungsverwaltung genutzten Verfahren, Dienstanweisungen und Vordrucke einer Überarbeitung unter Datenschutzaspekten zuzuführen.

In diesem Zusammenhang wurden unter anderem die Projekte „Online-Antragstellung" und „KomKo" (Kommunale Kooperation - Auskunfts- und Beratungsverfahren Schwerbehindertengesetz) vorgestellt. Außerdem sind bei zwei Versorgungsämtern Kontrollbesuche durchgeführt worden, die schwerpunktmäßig der Sichtung der in diesen Versorgungsämtern genutzten Verfahren, der vorhandenen Dienstanweisungen und der Vordrucke dienten. Insgesamt war danach ein **erheblicher Nachholbedarf** der Versorgungsverwaltung **in Sachen Datenschutz** festzustellen. Im Rahmen der Kontrollmitteilungen wurden zu verschiedenen Datenschutzthemen Lösungsvorschläge unterbreitet. In einer Reihe von Sitzungen der Arbeitsgruppe wurden ebenfalls verschiedene Datenschutzprobleme angesprochen und Lösungen diskutiert.

Auch wenn derzeit noch keine abschließenden Ergebnisse vorgestellt werden können, ist die Initiative des Sozialministeriums der richtige Weg eines präventiven Datenschutzes. Durch eine Vorabklärung kann letztlich ein datenschutzkonformes Verfahren konzipiert und können damit Datenschutzverstöße von vornherein weitgehend ausgeschlossen werden.

13.3 Call-Center einer gesetzlichen Krankenkasse

Eine gesetzliche Krankenkasse hat durch ein privates, von ihr beauftragtes Call-Center Versicherte in individuellen medizinischen Fragen beraten lassen. Um die „Anrufberechtigung" der Versicherten zu überprüfen und Anfragen abrechnen zu können, stellte die Krankenversicherung dem Call-Center auf einer CD-ROM Versichertendaten zur Verfügung. Eine Rechtsgrundlage hierfür bestand nicht.

Das Beratungsangebot des Call-Centers wurde auf dessen Homepage im Internet präsentiert. Die Beratung erfolgte telefonisch sowie mit E-Mail und beinhaltete allgemeine medizinische Informationen (beispielsweise zu Impfschutz auf Reisen oder zur Zahnpflege), individuelle Beratung durch Fachärztinnen und Fachärzte zu bestehenden Diagnosen sowie die Einholung weitergehender Informationen von Spezialkliniken zur Erstdiagnose und zu Behandlungsalternativen.

Datenschutzrechtliche Probleme ergaben sich dabei in mehrfacher Hinsicht.

Für die Weitergabe der Versichertendaten an das Call-Center bestand **keine Rechtsgrundlage**. Eine Datenverarbeitung im Auftrag nach § 80 Sozialgesetzbuch, Fünftes Buch - Gesetzliche Krankenversicherungen - (SGB V), schied aus, da die Krankenversicherung nicht mehr allein die Verantwortung für die Datenverarbeitung trug und die Tätigkeit des Call-Centers weit über eine reine Unterstützungsleistung für die Krankenkasse hinausging (siehe hierzu auch die „Orientierungshilfe Datenverarbeitung im Auftrag", abrufbar unter www.lfd.nrw.de). Vielmehr wurde dem Call-Center tatsächlich eigenverantwortlich eine Aufgabe übertragen. Dem stand jedoch § 284 Abs. 3 SGB V entgegen, der abschließend regelt, zu welchen Zwecken Sozialdaten von den gesetzlichen Krankenversicherungen erhoben und verarbeitet werden dürfen. Die telefonische Erteilung individueller medizinischer Auskünfte an ratsuchende Versicherte durch Ärzte und Ärztinnen eines privaten Call-Centers gehört nicht dazu.

Darüber hinaus bestand infolge der sehr tiefgehenden und individuellen telefonischen Beratung - auch im Widerspruch zu arztrechtlichen Vorschriften - die Gefahr der Erhebung und Speicherung unrichtiger Gesundheitsdaten.

Die Gespräche mit den Betreibern des Call-Centers und der Krankenkasse führten zur **Rückgabe der Versichertendaten** an die Krankenkasse und zur **Beschränkung des Beratungsangebotes** des Call-Centers auf allgemeine medizinische Hinweise. Zur Zeit suchen die Betreffenden nach technischen und rechtlichen Wegen, die medizinische Beratung in privaten Call-Centern datenschutzkonform zu gestalten.

Die weitere Entwicklung medizinischer Beratungsangebote im Internet und durch Call-Center wird kritisch zu begleiten sein. Der Schutz der Sozialdaten hat höchste Priorität.

13.4 Schweigepflichtentbindungserklärung von privaten Versicherungen

Viele der von privaten Versicherungen verwendeten Formulare für eine Ermächtigung zur Befreiung von der Schweigepflicht weisen datenschutzrechtliche Mängel auf.

Beschwerden von Bürgerinnen und Bürgern haben gezeigt, dass die Formulare zur Schweigepflichtentbindungserklärung dem Recht auf informationelle Selbstbestimmung der Betroffenen durchweg nur **unzureichend** Rechnung tragen.

Beispielsweise enthalten einige Formulare folgenden Text: *„Ich ermächtige die Versicherung, Auskünfte zur Prüfung möglicher Leistungsansprüche wegen Berufsunfähigkeit bei Ärzten, Zahnärzten, Krankenhäusern, sonstigen Krankenanstalten, anderen Personenversicherern und Behörden einzuholen"*. Abgesehen davon, dass nicht ohne weiteres verständlich ist, was unter „möglichen" Ansprüchen zu verstehen ist, ist die bloße Aufzählung der „Auskunftstellen", insbesondere die Verwendung des Begriffs „Behörden" zu **unbestimmt**. Der Begriff „Behörden" umfasst grundsätzlich auch Sozialversicherungsträger. Für diese bestimmt jedoch § 67b Abs. 2 SGB X, dass die betroffene Person im Einzelfall in eine Offenbarung eingewilligt haben muss. Somit sind in diesem Fall separate Einwilligungserklärungen der Betroffenen in die Datenübermittlung einzuholen. Zur Vermeidung von Missverständnissen sowie zur Wahrung des Bestimmtheitsgrundsatzes sollte deshalb bereits in der Schweigepflichtentbindungserklärung hinter dem Wort „Behörden" der Zusatz „mit Ausnahme von Sozialversicherungsträgern" eingefügt werden. Es muss **genau dargelegt** werden, wann und in welchem Umfang bei welcher Institution die Ermächtigung gelten soll. Den Versicherten muss anhand des Formulars sowohl die voraussichtliche Zeitdauer der Prüfung selbst als auch der zeitliche Umfang, der der Prüfung zugrundegelegt wird, deutlich werden. Die oben zitierte Formulierung lässt vollkommen offen, ob beispielsweise bereits Jahre zurückliegende Erkrankungen oder Diagnosen oder längst geheilte Krankheiten im Rahmen der Prüfung Berücksichtigung finden oder nicht. Die versicherte Person ist so nicht in der Lage, das Ausmaß ihrer Ermächtigung vor Abgabe derselben abzuschätzen.

Häufig findet sich in Versicherungsformularen auch die Formulierung: *„Ich ermächtige die Versicherung, Auskünfte zur Prüfung möglicher Leistungsansprüche ... bei allen Ärzten, Krankenhäusern und Krankenanstalten, bei*

denen ich in Behandlung war oder sein werde...". Auch durch diese Formulierung ist der **Datenverarbeitungszeitraum** (selbst unter Berücksichtigung des Interesses der Versicherungen an einer umfassenden Leistungsprüfung) **zu weit bemessen**. Es besteht die Gefahr, dass in diesem Zusammenhang lang zurückliegende Erkrankungen, die als geheilt gelten oder bei denen keine Gefahr des erneuten Auftretens besteht, wieder hervorgeholt werden, obwohl die betroffene Person sie als abgeschlossen betrachtet und sich nicht mehr mit ihnen auseinandersetzen will. Dies ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Hinzu kommt, dass die betroffene Person im Zeitpunkt der Abgabe der Erklärung noch überhaupt nicht erkennen kann, ob sie nicht in Zukunft an Krankheiten leidet, hinsichtlich derer sie ganz oder teilweise - aus Gründen des Schutzes ihrer persönlichen Intimsphäre oder aus Schamgefühl - nicht möchte, dass die Versicherung hiervon über eine Anfrage bei der sie behandelnden Ärztin oder dem Arzt Kenntnis erlangt. Dies kann insbesondere dann der Fall sein, wenn die Arztrechnung ohne Inanspruchnahme der Versicherung beglichen wird, da nach Einschätzung der versicherten Person der mögliche Schaden, der aus einem Bekanntwerden solcher medizinischen Daten außerhalb der Arztpraxis entstehen kann, höher zu bewerten ist als der finanzielle Schaden, der ihr aus der Nicht-Inanspruchnahme der Versicherung entsteht.

Ebenso sind die Erkrankungen von einer **Kenntnisnahme der Versicherung ausgeschlossen**, deren Unkenntnis die Versicherung selbst, beispielsweise durch ihr Bonus-System, herbeigeführt hat. Wenn eine Krankenversicherung die Nicht-Inanspruchnahme innerhalb eines Versicherungsjahres durch Rückerstattung mehrerer Monatsbeiträge prämiert, kann sie nicht gestützt auf eine zu Beginn der Versicherung unterschriebene Einwilligungserklärung gleichwohl medizinische Daten aus Erkrankungen innerhalb dieses Jahres verlangen. Trotz des Wortlauts der Einwilligungserklärung wäre die konkrete **Datenanforderung nicht zulässig**, da sie zur Aufgabenerfüllung der Krankenversicherung nicht erforderlich ist.

Wie diese Beispiele zeigen, muss den betroffenen Versicherten zumindest die **Tragweite** ihrer Erklärung auch für die Zukunft im Wesentlichen **erkennbar sein**, das heißt, sie müssen übersehen können, wie weit ihre Erklärungen in zeitlicher Hinsicht reichen.

Im Übrigen fehlt es auch an einer überzeugenden Erklärung für die Notwendigkeit einer Befugnis der Versicherungen, von einer zeitlich unbeschränkten Datenerhebungsbefugnis Gebrauch zu machen. Dass die Schweigepflichtentbindungserklärung grundsätzlich freiwillig abgegeben wird, rechtfertigt keine andere Beurteilung. Auch bei Einholung einer freiwilligen Erklärung ist die betroffene Person über alle wesentlichen Gesichtspunkte aufzuklären, da nur eine **informierte Erklärung** („informed consent") datenschutzrechtlich wirksam ist.

Besonders problematisch ist auch, dass extrem sensiblen medizinischen Informationen nicht Rechnung getragen wird. Die Abrechnung einer Grippeerkrankung erfolgt derzeit auf der Grundlage derselben, einmal in der Vergangenheit erteilten Einwilligungserklärung wie die Abrechnung einer Aids-Erkrankung. So ist in der Schweigepflichtentbindungserklärung oft auch nur von „Gesundheitsverhältnissen" die Rede, ohne dass zwischen körperlichen und psychischen Gesundheitsverhältnissen unterschieden wird. Auch auf diese Weise wird die versicherte Person im Unklaren über die Dimension der Datenübermittlung gelassen. Letzteres ist mit dem datenschutzrechtlich zu beachtenden **Transparenzprinzip** nicht zu vereinbaren. Den Betroffenen sollte bereits anhand des Formulars unmissverständlich klar sein, dass sich die Datenverarbeitung auf psychische und/oder physische Gesundheitsverhältnisse erstreckt. Dagegen spricht auch nicht § 34 Versicherungsvertragsgesetz (VVG), wonach die Versicherung nach Eintritt des Versicherungsfalls verlangen kann, dass die versicherte Person jede Auskunft erteilt, die zur Feststellung des Versicherungsfalls oder des Umfangs der Leistungspflicht der Versicherung erforderlich ist. Die **Auskunftspflicht** der versicherten Person besteht nur in den Grenzen der Erforderlichkeit. Kommt es im Rahmen der Leistungsprüfung beispielsweise allein auf die körperliche Verfassung der versicherten Person an, ist es nicht erforderlich, dass die Versicherung pauschal Auskunft über die „Gesundheitsverhältnisse" der Betroffenen erlangt. In diesem Fall muss es der versicherten Person möglich sein, ihre Auskunft oder die Ermächtigung der Versicherung zum Einholen von Auskünften auf Daten, die die körperliche Konstitution betreffen, zu **beschränken.** Auch bei später auftretenden besonders problematischen Erkrankungen muss unter Erläuterung der beabsichtigten Datenverarbeitung erneut die ausdrückliche Einwilligung hierzu eingeholt werden.

Die bisherige Einwilligungserklärung per Vertragsformular berücksichtigt außerdem nicht, dass beispielsweise nach § 10 Abs. 2 2. Halbsatz der

Berufsordnung für Ärztinnen und Ärzte eine Einsichtnahme der Patientinnen und Patienten in die Teile der Krankenunterlagen ausgeschlossen ist, die subjektive ärztliche Eindrücke oder Wahrnehmungen enthalten. Die Einwilligungserklärung der Versicherung unterscheidet ihrem Wortlaut nach hier nicht, so dass die betroffene Person, ohne diese Konsequenz auch nur zu ahnen, Daten zur Unterrichtung der Versicherung freigibt, zu denen sie selbst nach der Satzung der Ärztekammern keinen Zugang hat. Eine Einwilligungserklärung ohne eine solche Differenzierung ist im Ergebnis unwirksam.

Diese Fragen werden zur Zeit zwischen den Datenschutzbehörden und den Versicherungen in der Arbeitsgruppe „Versicherungswirtschaft" erörtert. Für die betroffenen Bürgerinnen und Bürger bleibt zu hoffen, dass es im Rahmen der Beratungen gelingt, die Versicherungen zu einer aufgeschlosseneren Haltung gegenüber den Datenschutzrechten ihrer Versicherten zu bewegen.

14 Gesundheit

Die Liste der Verstöße gegen das **Arzt-Patientengeheimnis in Arztpraxen** ist lang. Die Bestimmung der jeweils geltenden Berufsordnung ist dabei klar und eindeutig: Ärztinnen und Ärzte haben über das, was ihnen in Ausübung ihres Berufes anvertraut oder bekannt geworden ist, zu schweigen. In vielen Arztpraxen wird dies allerdings **unzureichend eingehalten**. Zahlreiche Beschwerden zeigen, dass Patientinnen und Patienten zunehmend nicht geneigt sind, dies länger hinzunehmen.

Ärztinnen und Ärzte haben weiter ihren Patientinnen und Patienten auf deren Verlangen **grundsätzlich Einsicht** in die sie betreffenden **Krankenunterlagen** zu gewähren; ausgenommen sind diejenigen Teile, die subjektive ärztliche Eindrücke oder Wahrnehmungen enthalten. Dieser Satz ist wortgleich in die novellierten Berufsordnungen (Berufsordnungen der Ärztekammern Nordrhein und Westfalen-Lippe) übernommen worden. Die Bemühungen um eine Erweiterung des Einsichtsrechts von Patientinnen und Patienten in ärztliche Dokumentationen (vgl. auch 15. Datenschutzbericht 2001 unter 11., S. 108) waren insofern leider erfolglos.

Patientinnen und Patienten bleibt damit, soweit sie von niedergelassenen Ärztinnen und Ärzten behandelt werden, weiterhin die Einsichtnahme in Niederschriften subjektiver ärztlicher Eindrücke oder Wahrnehmungen verwehrt. Dies wird dann besonders problematisch, wenn diese ärztlichen Eindrücke oder Wahrnehmungen wiederum im Rahmen von **Begutachtungsverfahren** den Gutachterinnen und Gutachtern zur Verfügung gestellt werden und damit Eingang in diese Gutachten finden. Allein an diesem Beispiel wird deutlich, welch schwerwiegenden Verstoß gegen das Recht auf informationelle Selbstbestimmung diese Regelung in den ärztlichen Berufsordnungen darstellt.

Zusätzlich ist es deshalb auch notwendig bei **Schweigepflichtentbindungserklärungen,** die von den Betroffenen aus den verschiedensten Gründen gefordert werden, diese Teile der ärztlichen Unterlagen, die den Betroffenen nach der derzeitigen Rechtslage nicht bekannt sein dürfen, ausdrücklich auszunehmen.

Das ebenfalls dringend zu überarbeitende **Gesundheitsdatenschutzgesetz** Nordrhein-Westfalen (GDSG NW), das in erster Linie für Krankenhäuser gilt, stellt die Gewährung der Einsichtnahme in subjektive Daten und Aufzeichnungen im Rahmen der Behandlung dem ärztlichen Ermessen

anheim. Eine Durchsetzungsmöglichkeit, eben diese Teile der Patientenakte einzusehen, haben die Betroffenen damit zwar direkt nicht, wohl aber Anspruch auf eine **nachvollziehbare Begründung**, warum in ihrem Falle diese Daten zurückgehalten werden. Als Ermessensentscheidung ist die Verweigerung der Auskunft und Akteneinsicht einer, wenn auch nur eingeschränkten, gerichtlichen Überprüfung zugänglich.

Im Übrigen haben die Betroffenen gegen die Ärztinnen und Ärzte einen **Auskunftsanspruch** nach § 34 BDSG, soweit personenbezogene Daten in einer automatisierten Datenverarbeitungsanlage oder in einer nicht automatisierten Datei verarbeitet, genutzt oder dafür erhoben werden; mögliche Auskunftsansprüche können sich aus dem Behandlungsvertrag mit den jeweiligen Ärztinnen und Ärzten ergeben.

14.1 Datenpool am Swimmingpool

In Kur- und Rehakliniken werden täglich zahlreiche komplette Patientendossiers von einer Einrichtung zur anderen transportiert, und zwar von den Patientinnen und Patienten selbst. Doch wohin mit den sensiblen Unterlagen beim Turnen, Schwimmen und während der Massage?

So wurden in einer Kurklinik die zu behandelnden Personen mit so genannten **Patientenbüchern** versehen, die bei jeder Anwendung oder Behandlung vorzulegen waren. Auf den Patientenbüchern standen gut lesbar Name, Geburtsdatum und vollständige Anschrift der Betroffenen, in den Patientenbüchern waren Angaben zu Größe, Gewicht, Blutdruck, Diagnosen sowie der vollständige Therapieplan verzeichnet. Nach Einsichtnahme durch das behandelnde Personal wurden die Patientenbücher auf allgemein zugänglichen Tischen oder sonstigen Ablagen vor dem jeweiligen Therapieraum (Gymnastikhalle, Schwimmbad) deponiert und verblieben dort während der Anwendung oder Behandlung mitunter stundenlang ohne Aufsicht.

Erfreulicherweise reagierte die Kurklinik umgehend auf die Empfehlungen und schaffte durch geeignete Maßnahmen Abhilfe. Auch sah sie Anlass, ihr Personal im Umgang mit Patientendaten noch einmal gründlich zu schulen.

14.2 Krankenhausentlassungsberichte an Krankenkassen

Bereits im 4. Tätigkeitsbericht 1982/83 unter 10 b, S. 50, wurde die Unzulässigkeit der Anforderung von Krankenhausentlassungsberichten durch Krankenkassen festgestellt. Im 10. Tätigkeitsbericht 1989/90 unter 5.10.2.2, S. 78 und im 14. Datenschutzbericht 1999 unter 7.5, S. 104, ist diese Feststellung auch unter Beachtung der zwischenzeitlich eingetretenen Rechtsänderung wiederholt worden. Gleichwohl setzten verschiedene gesetzliche Krankenkassen auch im Berichtszeitraum ihre rechtswidrige Praxis fort.

Allerdings ist es gelungen, eine große gesetzliche Krankenkasse davon zu überzeugen, nur noch medizinische Daten zur Vorlage beim medizinischen Dienst der Krankenversicherung (MDK) zu verlangen sowie durch technische und organisatorische Maßnahmen sicherzustellen, dass diese Daten nicht der Krankenkasse zur Kenntnis gelangen und außerdem die schriftliche Einwilligungserklärung der Versicherten so abzuändern, dass nur noch der Datenübermittlung an den MDK zugestimmt wird.

Nunmehr hat das Bundessozialgericht mit seinem Urteil vom 23. Juli 2002 - B 3 KR 64 01 R - klargestellt, dass die **Anforderung** von Krankenhausentlassungsberichten durch die Krankenkassen **unzulässig ist**, da die Einsicht in Behandlungsunterlagen weder zur Abrechnung mit den Leistungserbringern noch für die Beteiligung des MDK erforderlich ist. Eine solche Einsicht ist allein auf den MDK zu beschränken.

Damit ist jetzt höchstrichterlich entschieden, dass nur der MDK Zugriff auf die medizinischen Daten haben darf. Von den gesetzlichen Krankenkassen ist gesetzeskonformes Verhalten zu erwarten.

14.3 Kundendateien in Apotheken

Daten über Kundinnen und Kunden zu sammeln ist mittlerweile auch in Apotheken sehr verbreitet. Ebenso warf die Nutzung der Daten über das aus den Rezepten zu entnehmende Verordnungsverhalten der Ärztinnen und Ärzte datenschutzrechtliche Probleme auf.

Nach den bisher vorliegenden Fällen ist bei vielen Apotheken (und den Apothekenrechenzentren) derzeit noch ein bedauerlich geringes Datenschutzbewusstsein hinsichtlich der Datenschutzbelange ihrer

Kundinnen und Kunden, aber auch hinsichtlich der Datenschutzbelange der verordnenden Ärztinnen und Ärzte vorhanden.

- So glaubte beispielsweise ein Apotheker, er könne jedes Rezept für sich kopieren und über diese Daten dann frei verfügen.

- Eine Apothekenaufsichtsbehörde berichtete, dass in Apotheken ihres Aufsichtsbereiches verstärkt der Aufbau von Kunden-/Patientendateien festzustellen ist. Inhalte dieser Dateien sind unter anderem Name, Vorname, Geburtsdatum, Anschrift, Kassenzugehörigkeit, Hinweis auf Befreiung von Zuzahlungsverpflichtung, rezeptierte Arzneimittel und Zukäufe (Arzneimittel) ohne Rezept. Diese Daten werden - ohne schriftliche Einwilligung der Kundinnen und Kunden - von den Apotheken zum Zwecke der Ausstellung von Bescheinigungen über Zuzahlungsbeträge, für die Beratung und Information über Verkäufe in zurückliegenden Zeiträumen oder auch aus sonstigen Gründen, wie etwa zur **Versendung von Geburtstagsgrüßen**, zusammengetragen und verarbeitet. Die Apothekenaufsichtsbehörde wies in diesem Zusammenhang darauf hin, dass selbst der zuständige Apothekerverband für diese Datenverarbeitung lediglich eine Benachrichtigung der Betroffenen für ausreichend hielt.

- Eine Apothekenkammer gab die Information, dass Apothekerinnen und Apotheker zum Zwecke der Kundenbindung verschiedene Werbemittel unter Nutzung der Kundendaten verwenden. Die Rezeptdaten werden in eine Kundendatei übertragen und die so gewonnenen Daten von dem Apothekenbetrieb dafür genutzt, den Kundinnen und Kunden **Werbeschreiben** diverser Art zukommen zu lassen. Die Erhebung, Speicherung und Nutzung der personenbezogenen Daten wird mit den davon Betroffenen zuvor jedoch nicht besprochen.

- Nach Mitteilung einer Apothekenkammer sind auch so genannte **Kundenkarten** der Apotheken verbreitet. Mit diesen Kundenkarten sind Serviceangebote wie zum Beispiel der Interaktionscheck von Arzneimitteln oder die Rabattgewährung verbunden. Zwar würden bei der Beantragung der Karte die Kundinnen und Kunden darin einwilligen, dass ihre personenbezogenen Daten aus den Verschreibungen gespeichert und im Sinne der Kundenkarte genutzt würden. Von den Apothekenbetrieben würden die auf diese Art gewonnenen personenbezogenen Daten jedoch auch dazu benutzt, um

Kundinnen und Kunden Werbeschreiben oder Geburtstagsgratulationen zuzusenden.

- In einem anderen Fall wurde darauf hingewiesen, dass in einer Apotheke der Bereich, in dem üblicherweise Beratungsgespräche und Arzneimittelausgaben erfolgten, von einer **Videokamera mit Mikrofon** überwacht werde. Die Nutzung dieser sensiblen Daten etwa auch für Schulungszwecke des Personals (Steigerung der Effizienz von Verkaufsgesprächen) sei möglich.

- Auch die Bestellung von Arzneimitteln durch Apotheken über das **Internet** unter Offenlegung der personenbezogenen Daten der jeweils betroffenen Person wirft Datenschutzfragen nach der Erforderlichkeit einer solchen Datenverarbeitung und nach der Datensicherheit bei der Übertragung solcher Daten durch das Internet auf.

- Durch Auswertung der Rezeptdaten in Apothekenrechenzentren wurde das Verordnungsverhalten der verschreibenden Ärztinnen und Ärzte im Einzelnen genau analysiert und diese Analysen **Pharmaunternehmen** zur Verfügung gestellt. Diese nutzten die Auswertungen für gezielte **Werbeaktivitäten** gegenüber den Ärztinnen und Ärzten.

Allen dargestellten Beispielen ist gemeinsam, dass die aufgezeigte Verarbeitung von Kundendaten **jeweils rechtswidrig** und damit unzulässig ist. Zur Frage der Verarbeitung von Kundendaten in Apotheken (und in Apothekenrechenzentren) ist generell auf Folgendes hinzuweisen:

Die zulässige Verarbeitung personenbezogener Daten aus Verschreibungen für Patientinnen und Patienten der gesetzlichen Krankenkassen ist in § 300 Abs. 1 SGB V geregelt. Die oben dargestellten Nutzungen dieser Daten durch Apotheken geht dabei über den Rahmen von § 300 SGB V hinaus, und zwar auch über den möglichen Rahmen von Abs. 2 (Einschaltung von Rechenzentren, Möglichkeiten der Datenverarbeitung durch diese Rechenzentren). Eine **Erlaubnisnorm** für die Nutzung und weitere Verarbeitung dieser Daten für die dargestellten Zwecke **liegt nicht vor**.

Die Regelung in § 300 SGB V ist insoweit bereichspezifisch abschließend bezogen auf die Verarbeitung von Daten der gesetzlich versicherten Personen. Soweit daher Apotheken solche Daten generell für diese anderen Zwecke nutzen, wäre die Einholung einer Einwilligung nicht mehr eine

Erlaubnis für eine Datenverarbeitung im Einzelfall, sondern vielmehr die Einrichtung eines generellen Verfahrens zur **zweckändernden Nutzung** und weiteren Verarbeitung von Versichertendaten, mit der die Zweckbestimmung des Gesetzes in § 300 SGB V verändert und faktisch aufgehoben würde. Die Entscheidung des Gesetzgebers in dieser Weise abzuändern, dazu sind die Apotheken jedoch **nicht befugt**. Die Zulassung einer solchen weiteren Datenverarbeitung ist daher durch § 300 SGB V ausgeschlossen.

Die bei den Apotheken vorhandenen Daten aus der Erledigung von Verschreibungen, die den gesetzlichen Krankenkassen zu Abrechnungszwecken zugeleitet werden, können deshalb beispielsweise auch nicht zur Gewinnung von Daten für die Anfertigung der Kundenkarten genutzt werden.

Die Anfertigung von **Kundenkarten** setzt beispielsweise vielmehr eine **eigenständige Datenerhebung** der Apotheken bei ihren Kundinnen und Kunden voraus, bei der die geplanten Datenverarbeitungszwecke abschließend aufgezeigt und erläutert werden müssen (Transparenz der Datenverarbeitung). Weiter muss den Kundinnen und Kunden zweifelsfrei deutlich gemacht werden, dass die Datenerhebung völlig unabhängig von der Ausführung der Verschreibung ist und dass der einzelnen Person in dieser Hinsicht keinerlei Nachteile drohen, wenn sie auf die Anlage einer Kundenkarte verzichtet. Insoweit muss echte **Freiwilligkeit** vorliegen, die insbesondere einschließt, auf einzelne Serviceleistungen aus der Kundenkarte (jetzt oder später) problemlos verzichten zu können, wie beispielsweise auf die Zusendung von Werbeschreiben und Geburtstagsgratulationen. Auch die übrigen Voraussetzungen des § 4a BDSG zur Einwilligung müssen von der jeweiligen Apotheke beachtet werden.

Durch die Einholung der konkreten (wirksamen) Einwilligungserklärung ist der Rahmen der **zulässigen Verarbeitung** der so gewonnenen Daten dann allerdings **abschließend definiert**. Der Apotheke ist es nach Abgabe einer schriftlichen Einwilligungserklärung der Betroffenen nicht mehr möglich, nachträglich einseitig den Rahmen dieser Erklärung zu erweitern und eine zusätzliche Datenverarbeitung zu weiteren Zwecken vorzunehmen. Wegen Fehlens einer für diese zusätzliche Datenverarbeitung wirksamen Einwilligungserklärung wäre die Datenverarbeitung der Apotheken für diese zusätzlichen Zwecke stets rechtswidrig und deshalb unzulässig.

Die Apothekenkammern bleiben aufgerufen, für mehr Datenschutz gegenüber den Kundinnen und Kunden in Apotheken (und in Apothekenrechenzentren) zu sorgen. Allerdings ist nicht zu verkennen, dass auch die betroffenen Kundinnen und Kunden durch ein bewusstes Einfordern der Gewährleistung ihrer Datenschutzbelange durch die Apotheken selbst zu einem steigenden Datenschutzbewusstsein bei den Apotheken ganz erheblich beitragen können.

14.4 Patientendatenmissbrauch durch Apotheken und deren Rechenzentren

Im Berichtszeitraum ist ein bundesweiter Missbrauch von Patientendaten in Apotheken und Apothekenrechenzentren aufgedeckt worden, an dem auch viele der nordrhein-westfälischen Apotheken beteiligt sind.

Apotheken rechnen in der Regel nicht mehr selbst mit den jeweiligen Krankenkassen ab, sondern nehmen hierfür die Dienste von Apothekenrechenzentren in Anspruch. Die Rezepte werden an die Rechenzentren geleitet, die dann die Rezeptdaten elektronisch aufbereiten und den jeweiligen Krankenkassen zusenden. Die Kostenerstattung wird nur noch zwischen den Rechenzentren und den jeweiligen Krankenkassen abgewickelt. Die Apotheken erhalten ihre Kosten vorab von den Rechenzentren erstattet, abzüglich einer Bearbeitungsgebühr.

Die Inanspruchnahme von Rechenzentren zur Arzneimittelabrechnung lässt § 300 Abs. 2 Sozialgesetzbuch, Fünftes Buch - Gesetzliche Krankenversicherung - (SGB V) ausdrücklich zu. Nach dieser Vorschrift *„können die Apotheken und weitere Anbieter von Arzneimitteln zur Erfüllung ihrer Verpflichtung Rechenzentren in Anspruch nehmen; die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden."*

In letzter Zeit sind die Rechenzentren dazu übergegangen, die Rezeptdaten über den Zweck der Abrechnung mit den Krankenkassen hinaus auch für **andere Zwecke** der jeweiligen Apotheke auf CD oder im Online-Abruf zur Verfügung zu stellen. Die so genannte **Apotheken-CD** ermöglicht eine Katalogisierung der Daten nach verschiedenen Kriterien. Beispielsweise sind die Apotheken mit Hilfe der CD in der Lage, **sämtliche**

Patientendaten beliebig miteinander zu **kombinieren**. Die Verschreibungspraxis einzelner Ärztinnen und Ärzte lässt sich nach Medikamenten sortiert aufrufen, wobei auch eine Auswertung nach speziellen Medikamenten erfolgen kann. So können etwa personenbezogene **Rauschmittellisten** ebenso erstellt werden wie eine **Umsatzstatistik** für einzelne Ärztinnen und Ärzte. Die Apotheken können auf diese Weise erkennen, wer welche Patientinnen oder Patienten behandelt und welche Patientinnen oder Patienten einer bestimmten Region zu welcher Ärztin oder zu welchem Arzt gehen.

Diese elektronische Aufbereitung der Rezeptdaten (Identitätsdaten sowie die verschriebenen Arzneimittel) wird von § 300 Abs. 2 SGB V nicht mehr gedeckt. Zum einen geht eine Datenkatalogisierung über den eigentlichen **Zweck der Abrechnung** mit den Krankenkassen **weit hinaus** und wird daher von § 300 Abs. 2 Satz 2, 1. Halbsatz SGB V, wonach *„die Rechenzentren die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen dürfen"*, nicht mehr erfasst. Zum anderen kann auch § 300 Abs. 2, 2. Halbsatz SGB V, wonach *„anonymisierte Daten auch für andere Zwecke verarbeitet und genutzt werden dürfen"*, die Erstellung der Apotheken-CD nicht legitimieren. Selbst wenn eine Anonymisierung der Rezeptdaten erfolgte, handelte es sich bei der Datenkatalogisierung um eine zumindest **arztbezogene Auswertung**. Eine derartige Datenverarbeitung ist jedoch ausweislich Nr. 119 b zu § 300 SGB V der amtlichen Begründung der Bundesregierung zu ihrem Entwurf eines Gesetzes zur Reform der Gesetzlichen Krankenversicherung (GKV-Gesundheitsreform 2000) ausgeschlossen. Unter Nr. 119 b zu 300 SGB V heißt es: *„(....) Mit dieser Regelung wird den Rechenzentren die Verarbeitung und Nutzung anonymisierter Abrechnungsdaten erlaubt, z.B. für berufsspezifische Zwecke der Apotheker. Eine versicherten- oder arztbezogene Auswertung der Daten bleibt ausgeschlossen"*.

Die Erstellung der CD sowie der Online-Abruf **entbehren** somit **jeglicher Rechtsgrundlage**. Diese kann auch nicht durch entsprechende Einwilligungen der Betroffenen herbeigeführt werden, da § 300 Abs. 2 SGB V eine abschließende Gesamtregelung für die Datenverarbeitung bei der Arzneimittelabrechnung unter Zuhilfenahme von Rechenzentren darstellt. Die Zulässigkeit einer Datenverarbeitung aufgrund einer Einwilligung gemäß § 4a BDSG würde die bereichsspezifische Regelung des § 300 Abs. 2 SGB V unterlaufen. Daher kann die Datenverarbeitung im Rahmen der

Arzneimittelabrechnung nicht zur Disposition der Betroffenen stehen, so dass ein Rückgriff auf § 4a BDSG ausgeschlossen ist.

Es ist darauf hinzuwirken, dass der Vertrieb der Apotheken-CD sowie das Bereithalten der Daten für den Online-Abruf unterbleibt und die bereits vertriebenen CDs von den entsprechenden Apotheken zurückverlangt werden.

15 Ausländerinnen und Ausländer

Die datenschutzrechtliche Situation von Ausländerinnen und Ausländern wird sich erheblich verschlechtern. Abgesehen von der Einführung maschinenlesbarer Dokumente über den Aufenthaltsstatus sind etwa nach dem Terrorismusbekämpfungsgesetz im ausländerrechtlichen Verfahren wie auch im Asylverfahren **Aufzeichnungen von Sprachtests** zur Identitätsfeststellung zulässig, die bis zu zehn Jahre (im Asylverfahren gerechnet ab dessen Abschluss) aufbewahrt werden dürfen. Hierdurch dürfte allerdings weniger eine Bekämpfung des internationalen Terrorismus bewirkt werden als vielmehr eine vom Gesetzgeber erhoffte Feststellung der Herkunft einer Ausländerin oder eines Ausländers, um gegebenenfalls zu einem späteren Zeitpunkt deren oder dessen Abschiebung zu erleichtern. Abgesehen von der Frage der Tauglichkeit dieser Sprachtests (sie lassen kaum zweifelsfrei auf eine Staatsangehörigkeit schließen) ist zu bedenken, dass hier unter dem Vorwand der Terrorismusbekämpfung eine Erleichterung der täglichen Arbeit der Ausländerbehörden durchgesetzt worden ist, die als solche unter dem Gesichtspunkt der Verhältnismäßigkeit einer **strengeren Beurteilung** bedurft hätte. Gleiches gilt auch für zahlreiche weitere gesetzliche Neuregelungen, so für die Einführung neuer Tatbestände, bei deren Vorliegen eine **Identitätssicherung** vorgenommen werden kann, und für die **Übermittlung** von durch die Auslandsvertretungen im Visumverfahren erhobenen Daten an den Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz, den Militärischen Abschirmdienst, das Bundes- und das Zollkriminalamt zur Feststellung von Gründen, die der Erteilung eines Visums entgegenstehen. Die genannten Behörden dürfen die so erhaltenen Daten auch für ihre eigenen Zwecke speichern und nutzen. Auch das **Ausländerzentralregister** darf nun eine erheblich umfassendere Datenmenge über eine Ausländerin oder einen Ausländer speichern und unter erleichterten Bedingungen anderen Behörden den **Zugriff** auf diese Daten **gewähren** - eine datenschutzrechtlich äußerst bedenkliche Weichenstellung. Mit dem Argument der Terrorismusbekämpfung hat der Gesetzgeber einen weiteren großen Schritt dahin getan, Ausländerinnen und Ausländer „gläsern" werden zu lassen.

Durch das Terrorismusbekämpfungsgesetz haben auch weitere **biometrische Merkmale in Ausweisdokumenten** von Ausländerinnen und Ausländern Eingang in das Ausländer- und das Asylverfahrensgesetz gefunden. So wurde die Möglichkeit der Aufnahme biometrischer Merkmale

von Fingern, Händen oder Gesicht in Ausweispapiere von Ausländerinnen und Ausländern geschaffen (zu Pässen und Personalausweisen von Deutschen siehe unter 12). Im Vergleich zur Rechtslage bei deutschen Staatsangehörigen bestehen gewichtige Unterschiede: Während bei Ausweisen deutscher Staatsangehöriger die Umsetzung der Maßnahmen einem vom Gesetzgeber zu erlassenden Bundesgesetz vorbehalten ist, sollen die Einzelheiten für die Dokumente von Ausländerinnen und Ausländern lediglich im Wege einer **Rechtsverordnung** durch die Exekutive geregelt werden. Das Grundrecht auf informationelle Selbstbestimmung ist jedoch ein Menschenrecht und gilt daher für ausländische Mitbürgerinnen und Mitbürger in gleichem Maße wie für Deutsche. Ein derart wesentlicher Eingriff in die Persönlichkeitsrechte der Ausländerinnen und Ausländer müsste vom **Gesetzgeber selbst** entschieden werden. Im Gegensatz zu den deutsche Bürgerinnen und Bürger betreffenden Regelungen findet sich darüber hinaus im Ausländer- und im Asylverfahrensgesetz **kein Verbot der Einrichtung einer bundesweiten Referenzdatei.** Alle öffentlichen Stellen erhalten die Befugnis, sämtliche automatisch lesbaren Daten zur Erfüllung ihrer gesetzlichen Aufgaben zu speichern, zu übermitteln und zu nutzen. Damit sind jedoch die Zwecke, zu denen eine Datenverarbeitung zulässig sein soll, in keiner Weise hinreichend bestimmt. Dass der Umfang, in dem die gespeicherten Merkmale zukünftig zum Beispiel für polizeiliche Zwecke nutzbar gemacht werden, nicht absehbar ist, muss als **äußerst bedenklich** angesehen werden. Im Ergebnis ist durch die neuen ausländerrechtlichen Regelungen ein Verlust an Rechtsstaatlichkeit zugunsten einer zweifelhaften Verbesserung der Sicherheitslage zu beklagen.

Innenministerium und Ausländerbehörden beabsichtigen zudem, ein **elektronisches Abgleichverfahren** einzurichten, in welchem die aus aufgefundenen Ausweispapieren ersichtlichen Daten einschließlich biometrischer Daten aus den darin enthaltenen Lichtbildern in einer **bundesweiten Datenbank** gespeichert werden sollen. Bei Bedarf sollen diese Daten mit den Daten einer Person, deren Staatsangehörigkeit unklar ist und die vorgibt, kein Ausweisdokument zu besitzen, dann verglichen werden können. Ein solches Vorgehen findet weder im Ausländergesetz noch in sonstigen Gesetzesvorschriften eine rechtliche Grundlage.

16 Polizei

Nach dem 11. September 2001 ist bundesgesetzlich ein ganzes Bündel weiterer Verschärfungen der Sicherheitsgesetze beschlossen worden. Zum Entwurf eines Terrorismusbekämpfungsgesetzes des Bundes haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 24. - 26.10.2001 (Abdruck im Anhang, Nr. 8) darauf hingewiesen, dass sich alle neu erwogenen Maßnahmen daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich **zielführend** und **erforderlich** sind und ob sie den Grundsatz der **Verhältnismäßigkeit** einhalten. Abgelehnt wird insbesondere eine Ausdehnung von Auskunftspflichten und Ermittlungskompetenzen. Zwar sind gegenüber dem ersten Gesetzentwurf einige Korrekturen erfolgt, dennoch enthält das am 1. Januar 2002 in Kraft getretene Terrorismusbekämpfungsgesetz **erhebliche Einschränkungen** des Rechts auf **informationelle Selbstbestimmung** einer Vielzahl unbescholtener Bürgerinnen und Bürger. Die gesetzlichen Neuregelungen beinhalten weitreichende Eingriffsbefugnisse der Polizei- und Verfassungsschutzbehörden des Bundes. Erhebliche Zweifel bestehen, ob etliche der übereilt beschlossenen Befugnisregelungen eine angemessene und zielorientierte Reaktion darstellen und das Übermaßverbot hinreichend beachten.

Das Gesetz sieht überdies für Polizei und Nachrichtendienste zusätzliche erhebliche Eingriffs- und Datenverarbeitungsbefugnisse vor, die sensible Bereiche des Rechtsstaats wie die föderale Struktur der Polizei, die Unterscheidung von Strafverfolgung und Gefahrenabwehr und die Trennung von Polizei und Geheimdiensten empfindlich stören. So ist zum Beispiel das **Bundeskriminalamt** künftig befugt, bei sämtlichen öffentlicher oder nichtöffentlichen Stellen ohne nähere Begründung „Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen" zu erheben. Damit ist eine **Grauzone von Ermittlungen** eröffnet, die über die Zentralstellenfunktion des Bundeskriminalamts hinausgeht und die Länderzuständigkeit für die Gefahrenabwehr in Frage stellt. Den **Nachrichtendiensten** - und mittlerweile auch dem Verfassungsschutz auf Landesebene - sind umfangreiche **Auskunftsbefugnisse** gegenüber Banken, Post-, Telekommunikations-, Teledienst- und Luftfahrtunternehmen eingeräumt worden. Dabei soll es nicht darauf ankommen, ob sich Betroffene strafrechtlich verdächtig gemacht haben. Durch diese neuen Ermittlungsbefugnisse auf Gebieten, für die die Polizei zuständig ist, wird

das verfassungsrechtliche **Trennungsgebot** zwischen polizeilicher und nachrichtendienstlicher Tätigkeit **weiter aufgeweicht**. Weitreichende Befugnisse zur Datenerhebung, -übermittlung und -speicherung sind insbesondere im **Ausländerrecht** vorgenommen worden. Der Eindruck, dass für Ausländerinnen und Ausländer nur ein **Datenschutz 2. Klasse** besteht, wird durch die Fülle der neu eingeführten Überwachungsinstrumentarien bestärkt (siehe hierzu unter Nr. 15).

Erhebliche Bedenken bestehen überdies gegen die neu eingeführte Befugnis zur **Übermittlung von Sozialdaten** an Strafverfolgungsbehörden, soweit sie zur Durchführung von nach Bundes- oder Landesrecht zulässigen **Rasterfahndungen** erforderlich sind. Bisher ist nicht bekannt, dass Sozialleistungsträger einen bestimmten, im Rahmen einer Rasterfahndung vorgegebenen Merkmalkatalog zu übermittelnder Daten aus ihren Beständen überhaupt zusammengefasst ermitteln können. Die Normentauglichkeit ist damit nicht erwiesen.

Zu bedauern ist außerdem, dass vor dem Gesetzgebungsverfahren nicht überprüft wurde, welchen Sicherheitsgewinn die zahlreichen Antiterrorgesetze der letzten 20 Jahre gebracht haben und ob Vollzugsdefizite bei den Sicherheitsbehörden bestehen, die vorrangig auszuräumen gewesen wären. Zwar hat der Gesetzgeber der Forderung der Datenschutzbeauftragten des Bundes und der Länder entsprochen und eine **Befristung** des Bundesverfassungsschutz-, des MAD- , des G 10- und des Sicherheitsüberprüfungsgesetzes sowie des § 7 Abs. 2 des BKA-Gesetzes vorgesehen. Bestimmt wurde weiter, dass diese - ab dem 11. Januar 2007 wieder in ihrer am 31. Dezember 2001 maßgeblichen Fassung geltenden - Vorschriften vor Ablauf der Befristung zu evaluieren sind. Dies gilt jedoch nicht hinsichtlich der sonstigen zahlreichen und unbefristet in Kraft getretenen Neuregelungen. Eine Erfolgskontrolle der sonstigen umfangreichen Eingriffsbefugnisse des Terrorismusbekämpfungsgesetzes bleibt damit auf der Strecke.

Zur Ermittlung so genannter „Schläfer", die in Verbindung mit terroristischen Gewalttaten stehen, hat auch die nordrhein-westfälische Polizei eine bundesweit koordinierte **Rasterfahndung** durchgeführt. Die Polizei kann nach der geltenden Rechtslage zur Rasterfahndung von öffentlichen und nicht-öffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien verlangen, soweit dies zur **Abwehr einer gegenwärtigen Gefahr** für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer

Person erforderlich ist. Sie erfolgt durch automatisierten Abgleich der übermittelten Angaben mit anderen Datenbeständen und erstreckt sich auf bestimmte Merkmale (Rasterkriterien), vgl. § 31 Abs. 1 und 2 Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW). Als Trefferangaben werden nur die Daten ausgeworfen, auf die alle Merkmale zutreffen. Gegen Personen, die alle Rasterkriterien aufweisen, wird auf der Grundlage der polizeirechtlichen und strafprozessualen Vorschriften weiter ermittelt. Die Rasterfahndung setzt eine richterliche Anordnung voraus.

Auf der Grundlage eines Beschlusses des Amtsgerichts Düsseldorf vom 02. Oktober 2001 (151 Gs 4092/01) erfolgte die Erhebung und Auswertung von **Datenbeständen** aus dem Hochschulbereich, den Einwohnermeldeämtern und dem Ausländerzentralregister durch eine Arbeitsgruppe des mit der Durchführung der Rasterfahndung beauftragten Polizeipräsidiums Düsseldorf. Der gerichtliche Beschluss wurde durch das Oberlandesgericht Düsseldorf (Beschluss vom 08. Februar 2002 - 3 Wx 356/01) zwar insoweit bestätigt, als es - im Gegensatz zu Gerichten anderer Bundesländer - eine gegenwärtige polizeirechtliche Gefahr als Voraussetzung der Rasterfahndung als gegeben angesehen hat. Allerdings hat das Gericht auf Anträge von Beschwerdeführern mit deutscher Staatsangehörigkeit erkannt, dass die Rasterfahndung hier rechtswidrig erfolgt ist. Damit sind alle Betroffenen mit deutscher Staatsangehörigkeit zu Unrecht in die Rasterfahndung einbezogen worden.

Auch nachdem die eigentliche Rasterfahndung abgeschlossen ist und die erhobenen Datensätze (mitsamt den Datensätzen von deutschen Staatsangehörigen) bis auf etwa 11000 vernichtet worden sind, wird die weitere Nutzung dieser Daten im Zuge der laufenden polizeilichen Ermittlungen weiter im Auge behalten. Ebenso wie die Rasterfahndung als solche wegen der **Einbeziehung** einer **Vielzahl** unbescholtener und **unverdächtiger Personen** einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht und damit eine unter grundrechtlichen und rechtsstaatlichen Gesichtspunkten sehr problematische **Verdachtsschöpfungsmethode** darstellt, erweist sich auch die weitere Nutzung der aus ihr gewonnenen personenbezogenen Daten als bedenklich.

Bei den weiteren polizeilichen Ermittlungen übernimmt das Bundeskriminalamt eine zentrale und koordinierende Rolle, indem es die aus den Rasterfahndungen der Länder ermittelten Daten untereinander abgleicht. Dies ist jedoch problematisch, weil dem **Bundeskriminalamt keine Befugnis** zusteht, rasterfahndungsähnliche Maßnahmen zur Gefahrenabwehr

durchzuführen. Die Errichtungsanordnung für die Verbunddatei „Schläfer" enthält hierfür keine ausreichende Rechtsgrundlage.

Besonderes Gewicht ist bei den weiteren polizeilichen Maßnahmen daher auf eine **grundrechtssichernde Überprüfung** zu legen, ob der Zweck der Rasterfahndung erreicht ist oder sich zeigt, dass er nicht erreicht werden kann. In diesen Fällen sind die im Wege der Rasterfahndung gewonnenen Daten nach Maßgabe des § 31 Abs. 3 PolG NRW zu löschen. Das Polizeipräsidium Düsseldorf hat die insoweit erforderlichen Schritte zugesagt.

Vor diesem Hintergrund beabsichtigt das Innenministerium, im Rahmen einer **Novellierung des Polizeigesetzes** die **Eingriffsschwelle** für eine **Rasterfahndung zu senken** und unter anderem auf das Vorliegen einer gegenwärtigen Gefahr zu verzichten. Wegen der verfassungsrechtlich gebotenen strengen Anforderungsvoraussetzungen für eine Rasterfahndung sind hiergegen erhebliche Einwände geltend zu machen. Insbesondere angesichts der mit einer Rasterfahndung verbundenen **massenhaften Grundrechtseingriffe** und der - soweit bekannt - bisherigen Erfolglosigkeit solcher Maßnahmen liegt die Konsequenz nahe, zumindest im Polizeirecht ganz auf sie **zu verzichten**. Ebenfalls abgelehnt wird die geplante Neuregelung, im Rahmen der Rasterfahndung ergänzende Datenerhebungen durchzuführen. Dies könnte dazu führen, dass die richterliche Anordnung unterlaufen würde, in der präzise und abschließend festzulegen ist, welche Daten wo erhoben werden dürfen.

Die umfangreichen Auskunftsbefugnisse des Bundesamtes für Verfassungsschutz wurden mit dem Terrorismusbekämpfungsgesetz auch den Verfassungsschutzbehörden der Länder unter dem Vorbehalt einer gleichwertigen Verfahrensregelung und -kontrolle eingeräumt. Dementsprechend wurde das **Verfassungsschutzgesetz NRW** dem Bundesverfassungsschutzgesetz angepasst. Im Gesetzgebungsverfahren war unter anderem darauf hinzuweisen, dass aus der Gesetzesbegründung keine Erforderlichkeit für die **weitreichenden Erhebungsbefugnisse** der Verfassungsschutzbehörde erkennbar war.

Mit der Neufassung des Runderlasses zur **Führung von Kriminalakten** ist nach der bereits überarbeiteten Richtlinie für die Führung Kriminalpolizeilicher personenbezogener Sammlungen - KpS - (siehe hierzu 15. Datenschutzbericht 2001 unter 4, S. 72) der Datenschutz bei der polizeilichen Datenspeicherung weiter verbessert worden. Kriminalakten

beschränken sich auf die Speicherung von Angaben über Tatverdächtige sowie Beschuldigte in einem strafrechtlichen Ermittlungsverfahren oder über Verurteilte. Eine Kriminalakte darf nur geführt werden, wenn sich nach einer Prognose der Polizei oder eines Gerichtes ergibt, dass die Person auf Grund ihrer Persönlichkeit, der Art oder Ausführung der Straftat oder sonstiger Erkenntnisse erneut eine Straftat begehen könnte. Kriminalakten enthalten unter anderem erkennungsdienstliche Unterlagen, Auszüge aus dem Bundeszentralregister, personengebundene Hinweise auf besondere Gefährlichkeit, Suchtkrankheiten und psychische Störungen sowie Mitteilungen über verfahrensrechtliche Entscheidungen. Es ist allerdings nicht einzusehen, dass etwa Unterlagen über Vermisstenfälle oder Unterlagen und Anzeigen, die nicht von den Strafverfolgungsbehörden gefertigt wurden, in Kriminalakten aufbewahrt werden können. Sie sollten gesondert gespeichert werden. Diese und andere Vorschläge zur Änderung und Präzisierung einzelner Regelungen in dem Runderlass zur Führung von Kriminalakten sind jedoch leider **unberücksichtigt** geblieben.

Unbefriedigend ist ebenfalls, dass Auszüge aus dem **Bundeszentralregister** in der kriminalpolizeilichen Akte verbleiben, auch wenn die Eintragung über eine Verurteilung in dem Register bereits getilgt worden oder sie zu tilgen ist. Dies widerspricht dem Vorhalte- und Verwertungsverbot des § 51 Abs. 1 Bundeszentralregistergesetz, wonach bei Eintritt der Tilgungswirkung die Tat und die Verurteilung der betroffenen Person im Rechtsverkehr nicht mehr vorgehalten und nicht zu ihrem Nachteil verwertet werden dürfen. Insofern bedürfen die KpS-Richtlinien zur Vermeidung inhaltlich unrichtiger Datenspeicherungen durch die Polizei noch einer Korrektur.

Anlässlich des Weltwirtschaftsgipfels G 8 im Jahr 2001 in Genua ist im Zusammenhang mit den dazu im Vorfeld getroffenen Sicherheitsmaßnahmen einer Vielzahl von Bürgerinnen und Bürgern die Ausreise durch den Bundesgrenzschutz untersagt worden. Wie sich herausgestellt hat, waren die Betroffenen anlässlich dieses Gipfelereignisses in dem Informationssystem des Bundeskriminalamtes INPOL-BKA **zur Fahndung ausgeschrieben**. Die Zulässigkeit dieser Ausschreibungspraxis ist datenschutzrechtlich **bedenklich**, weil der geschützte Datenbestand „Landfriedensbruch und verwandte Straftaten" bei zeitlicher Aneinanderreihung von Gipfelereignissen mit der entsprechenden Freischaltung de facto zu einem Teil der offenen INPOL-Fahndung werden kann. Darüber hinaus muss sichergestellt sein, dass in dem Informationssystem nur wirklich gewalttätige Personen erfasst werden. Es

darf nicht vorkommen, dass Bürgerinnen und Bürgern, die etwa bei Demonstrationen offensichtlich nicht gewaltsam in Erscheinung getreten sind, die Ausreise aus Deutschland verweigert wird. Zu fordern ist deshalb insbesondere, dass der Antrag eines Landes auf Freischaltung des geschützten Bestandes „Landfriedensbruch" deutlich von einer Ausschreibung in INPOL zu unterscheiden ist.

Die Innenminister des Bundes und der Länder haben die Einrichtung spezieller **Verbunddateien** („Gewalttäter rechts", „Gewalttäter links" und „Straftäter politisch-motivierter Ausländerkriminalität") beschlossen. Die hiergegen von dem Bundesbeauftragten für den Datenschutz mit Unterstützung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geltend gemachten **Zweifel** an der **Erforderlichkeit** und **Verhältnismäßigkeit** dieser umfangreichen bundesweiten Dateien konnten bisher nicht ausgeräumt werden.

16.1 Opferschutz im Polizeigesetz

Zum Januar 2002 wurde das Polizeigesetz des Landes Nordrhein-Westfalen in einem wichtigen Punkt zum Opferschutz geändert.

Um den Opfern **häuslicher Gewalt** wirksamer als bisher polizeilichen Schutz zu gewähren, wurde zeitgleich mit dem ab 01. Januar 2002 gültigen Gewaltschutzgesetz des Bundes das Polizeigesetz um einen § 34a ergänzt. Damit wurden die polizeirechtlichen Befugnisse geschaffen, eine gewalttätige Person vorübergehend für einen bestimmten Zeitraum aus der Wohnung der gefährdeten Person zu verweisen. Einen nachhaltigen Beitrag zum Opferschutz soll zusätzlich die Beratung der Opfer leisten.

Der Forderung in dem Gesetzgebungsverfahren, dass die Daten des Opfers nicht gegen seinen Willen an Beratungseinrichtungen übermittelt werden dürfen, wurde Rechnung getragen. Die Polizei setzt die Neuregelung in der Weise um, dass der Kontakt mit einer geeigneten Beratungseinrichtung nur mit Einwilligung des Opfers durch Bekanntgabe des Namens, der Anschrift und der Telefonnummer möglich ist.

16.2 Unfallnachsorge bei Straßenverkehrsunfällen

Im Rahmen einer Unfallnachsorge bei Straßenverkehrsunfällen mit Kindern sollten den beteiligten Kindern durch die Polizei Maßnahmen

zur Verkehrserziehung angeboten werden. Datenschutzrechtlich problematisch ist dabei die Speicherung und Nutzung der im Rahmen der repressiven polizeilichen Unfallbearbeitung erhobenen Daten für eine Kontaktaufnahme im Rahmen einer Unfallnachsorge.

Diese Daten dürfen außer im Fall der Einwilligung der Erziehungsberechtigten nur für den Zweck verwendet werden, zu dem sie erhoben worden sind. Gemeinsam mit der Polizei wurde eine **datenschutzkonforme** Möglichkeit erarbeitet, die **Verkehrserziehungsmaßnahmen** anzubieten. Während der Unfallbearbeitung hat die Polizei Kontakt mit den beteiligten Kindern (zum Beispiel bei einer Anhörung). Dabei kann sie die Erziehungsberechtigten mündlich oder durch Aushändigung eines Merkblattes über die Verkehrserziehung informieren und die Teilnahme anbieten. Die Erziehungsberechtigten können dann von sich aus auf die Polizei zugehen und ihr Kind zu einer solchen Maßnahme anmelden.

In diesen Fällen können die Daten der Kinder mit Einwilligung der Erziehungsberechtigten solange und soweit es für die Durchführung der Verkehrserziehung notwendig ist, gespeichert bleiben.

16.3 Ordnungspartnerschaft zwischen Polizei und privaten Sicherheitsdiensten

Die seit einiger Zeit in Nordrhein-Westfalen bestehenden so genannten Ordnungspartnerschaften zwischen Polizeibehörden, privaten Sicherheitsdiensten und anderen Stellen, sollen ein - allerdings nicht messbares - Sicherheitsbedürfnis von Bürgerinnen und Bürgern befriedigen und eine bürgerorientierte Polizeiarbeit verstärken. Darf die Polizei dabei bestimmte Ermittlungsaufgaben auf private Dritte übertragen?

Angestrebt wird mit einer Ordnungspartnerschaft insbesondere eine Verständigung der Verantwortlichen über eine enge Kooperation und Kommunikation zur Erhöhung der Sicherheit im kommunalen Bereich. Wie dies in der Praxis funktioniert, wurde anlässlich von Kontrollbesuchen bei einer Polizeibehörde und zwei privaten Sicherheitsdiensten überprüft. Dabei hat sich ergeben, dass eine **Zusammenarbeit** mit privaten Sicherheitsdiensten auf Grund der besonderen Aufgabenstellung der Polizei **problematisch werden kann**. Zwar bestand bei den Beteiligten Klarheit darüber, dass durch eine Ordnungspartnerschaft Rechte und Pflichten weder

begründet noch erweitert werden können. Dennoch war gegenüber der Polizeibehörde darauf aufmerksam zu machen, dass ihr als hoheitlich tätigem Ordnungspartner die besondere Verpflichtung obliegt, ständig darauf zu achten, dass die Grenzen der Kooperation nicht überschritten werden. Vernachlässigte die Polizei diese elementare Aufgabe, wäre unter Umständen mit Datenverarbeitungen im Übermaß und sonstigen unzulässigen Datenerhebungen und -speicherungen durch private Sicherheitsdienste zu rechnen. Eine von den polizeirechtlichen Vorschriften nicht gedeckte **Ausweitung der Informationsbeschaffung** durch andere institutionalisierte Einrichtungen neben der Polizei selbst gilt es auf Grund der historischen Erfahrungen der deutschen Vergangenheit dringend zu vermeiden. Kooperationserklärungen in Form solcher Ordnungspartnerschaften sind deshalb datenschutzrechtlich grundsätzlich problematisch.

Wenn auch im Grundsatz wegen des bislang nur sehr geringen Informationsflusses von den privaten Sicherheitsdiensten an die Polizei im Zeitpunkt der Untersuchung keine Besorgnis bestand, begegneten **einzelne Verfahrensweisen** der Polizeibehörde doch zum Teil erheblichen **datenschutzrechtlichen Bedenken**. Verschiedene in der Ordnungspartnerschaft festgelegte Kooperationsvereinbarungen waren zum einen viel zu allgemein gehalten, zum anderen waren nur Selbstverständlichkeiten formuliert. Insgesamt wird den bei den privaten Sicherheitsdiensten Verantwortlichen mit solchen Hinweisen nicht hinreichend deutlich, unter welchen Voraussetzungen der Polizei Informationen gemeldet werden sollen. Fragen wirft auch der Informationsweg an die Polizei über eine von privaten Sicherheitsdiensten gemeinsam betriebene Leitstelle auf. Datenschutzrechtlich **unzulässig** ist die **regelmäßige Übersendung** von Übersichten an die privaten Sicherheitsdienste („Gemeinsames tägliches Lagebild"), soweit aus diesen Unterlagen personenbezogene Daten erkennbar sind. Eine Änderung der Verfahrensweise wurde zugesagt. Darüber hinaus konnte den verantwortlichen Firmen das aus Rechtsstaatsgründen zu beachtende Erfordernis einer strikten Trennung der Aufgaben und Befugnisse der Polizei von den Tätigkeitsbereichen der privaten Sicherheitsdienste verdeutlicht werden. Die Grenzen einer Kooperation werden nach den bisherigen Feststellungen von den überprüften privaten Sicherheitsfirmen gegenwärtig beachtet.

Eine Ausweitung der bisher nur sporadisch erfolgenden Informationsflüsse birgt das Risiko einer Durchbrechung der rechtsstaatlich gebotenen Trennung zwischen polizeilichen und privaten Aufgaben. Vor diesem Hintergrund werden die Ordnungspartnerschaften auch weiterhin im Hinblick auf die Einhaltung des Datenschutzes kritisch zu beobachten sein.

16.4 Nur noch bargeldlose Zahlung von Verwarnungsgeldern - Anonymität dahin?

Nach den Plänen des Innenministeriums sollen betroffene Personen ein Verwarnungsgeld künftig nicht mehr in bar, sondern nur noch bargeldlos, per ec- oder Kreditkarte oder durch Überweisung bezahlen können. Damit würde die bisherige Praxis aufgegeben werden, ein Verwarnungsgeldverfahren anonym durchzuführen.

Das ist klar zu kritisieren, denn nur die **anonyme Abwicklung** des Verwarnungsgeldverfahrens entspricht dem Grundsatz der Datenvermeidung (§ 4 Abs. 2 Satz 1 DSG NRW). Bisher war es zur wirksamen Erteilung einer Verwarnung mit Erhebung eines Verwarnungsgeldes in keiner Weise erforderlich, bei der Barzahlung personenbezogene Daten der betroffenen Person zu verarbeiten.

Der Wegfall der anonymen Abwicklung eines Verwarnungsgeldverfahrens steht nicht im Einklang mit Wortlaut, Sinn und Zweck der Regelung des § 56 Abs. 2 Satz 1 Ordnungswidrigkeitengesetz (OWiG). Danach hat die betroffene Person eine **Wahlmöglichkeit** und kann das Verwarnungsgeld entweder sofort bezahlen oder innerhalb einer Frist bei der hierfür bezeichneten Stelle oder bei der Post zur Überweisung an diese Stelle einzahlen. Wird das Verwarnungsgeld sofort an Ort und Stelle bezahlt, ist das Verfahren abgeschlossen (§ 56 Abs. 4 OWiG). Eine sofortige Verfahrenserledigung ist mit den beabsichtigten bargeldlosen Zahlungsmöglichkeiten nicht garantiert. Erst mit dem Eingang der endgültigen Gutschrift auf dem Konto der Behörde wäre das Verfahren erledigt. Zudem hinterlassen die Betroffenen bei jeder bargeldlosen Zahlungsweise **Datenspuren**. Es ist davon auszugehen, dass hierbei Angaben über die Ordnungswidrigkeit nicht nur bei der Polizei gespeichert, sondern auch an Dritte (Abrechnungszentren, Kreditinstitute) übermittelt und dort gespeichert werden. Der Wegfall der Barzahlungsmöglichkeit und der sofortigen Verfahrenserledigung ist für die Betroffenen deshalb nachteilig. Das Innenministerium hält die vorgesehene Neuregelung

demgegenüber für zulässig und begründet sie mit ökonomischen Erwägungen.

Verwarnungsgeldverfahren sollten wie bisher auch anonym durchgeführt werden können. Der Grundsatz der Datenvermeidung und ökonomische Gesichtspunkte lassen sich durchaus vereinbaren.

17 Justiz

Das Strafverfahrensänderungsgesetz 1999 erforderte eine Überarbeitung der „Richtlinien für das Strafverfahren und das Bußgeldverfahren" (RiStBV) sowie der „Richtlinien über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung" (Anlage B zu den RiStBV). Gegenüber dem Justizministerium wurden zu mehreren Einzelfragen Änderungsvorschläge unterbreitet. Kritisch war etwa anzumerken, weshalb nicht auch die Voraussetzungen einer Auskunftserteilung an nicht anwaltlich vertretene Beschuldigte (§ 147 Abs. 7 Strafprozessordnung-StPO) in die RiStBV aufgenommen wurden. Hier sind Regelungen dazu notwendig, in welchen zu präzisierenden Ausnahmefällen eine **Auskunftsverweigerung** erfolgen darf. Zu begrüßen ist eine klarstellende Regelung der Aktenführung. Sie schreibt nunmehr einen besonders sensiblen Umgang mit **Lichtbildern von Verletzten** vor, die diese bei einer Gewährung von Akteneinsicht kompromittieren könnten. Die weiteren **Änderungsvorschläge** haben nicht oder nur teilweise Berücksichtigung gefunden. Die geänderte Fassung der RiStBV ist mit Wirkung vom 01. Juli 2002 in Kraft getreten.

Weitere Forderungen wurden zu Regelungen im Bereich der **Öffentlichkeitsfahndung** (Anlage B zu den RiStBV) erhoben, weil die Einschaltung von Publikationsorganen (Presse, Rundfunk, Fernsehen) ebenso wie die Nutzung öffentlich zugänglicher elektronischer Medien (insbesondere des Internet) wegen ihrer weiten Verbreitung und leichten Zugänglichkeit auch das Risiko der Verletzung des Grundrechts auf informationelle Selbstbestimmung bergen. Insbesondere sollten **potentielle Rufschädigungen** nicht verurteilter Tatverdächtiger berücksichtigt und der Begriff der eine Öffentlichkeitsfahndung ausschließenden „überwiegenden schutzwürdigen Interessen" von Zeuginnen und Zeugen (§ 131 a Abs. 4 StPO) auch insoweit näher konkretisiert werden. Schließlich wurden **kürzere Fristen** für die Überprüfung der Voraussetzungen einer Öffentlichkeitsfahndung im Internet gefordert, um möglichen schwerwiegenden Beeinträchtigungen Unschuldiger zu begegnen.

Die automatisierte Verarbeitung **personenbezogener Verfahrensdaten** bei den Staatsanwaltschaften soll nach den Planungen des Justizministeriums bis spätestens 31. Mai 2003 mit dem bereits in Schleswig-Holstein, Brandenburg, Hessen und Hamburg eingesetzten Verfahren MESTA („Mehrländer-Staatsanwaltschafts-Automation") erfolgen. Hierzu ist eine Errich-

tungsanordnung für automatisierte Dateien erforderlich (§ 490 StPO). Mit der vorgesehenen behördenspezifischen Neuregelung eröffnet sich die Chance, die seit langem bestehenden Probleme einer **unzureichenden Löschung** von Daten Unschuldiger in staatsanwaltschaftlichen Verfahrensregistern auszuräumen (siehe zuletzt 13. Datenschutzbericht 1995/96 unter 9.2, S. 72/73). Diese und andere Fragen wurden mit dem Justizministerium und der das Projekt entwickelnden Generalstaatsanwaltschaft Düsseldorf eingehend erörtert. Zu begrüßen ist, dass wesentliche datenschutzrechtliche Forderungen durch klarstellende oder ergänzende Bestimmungen in der Errichtungsanordnung sowie in der Dienstanweisung zum Datenschutz und zur Datensicherung beim Einsatz von IT-Geräten bei Justizbehörden des Landes Nordrhein-Westfalen (Rundverfügung des Justizministeriums vom 25. März 2002) berücksichtigt werden (etwa: abschließende Nennung möglicher Stellen, die Daten erhalten können, klare Vorgaben zur Verantwortlichkeit für die Datenlöschung). Einigkeit besteht im Ergebnis auch über das Erfordernis, spezielle Regelungen zur **Datensicherheit** in behördenbezogenen Dienstanweisungen zu treffen. Diese Verpflichtung folgt aus § 10 Abs. 3 DSG NRW, der ein zu dokumentierendes Sicherheitskonzept vorschreibt.

Anlässlich der Neufassung der **„Anordnung über Mitteilungen in Strafsachen"** (MiStra) im Jahre 1998 (siehe 14. Datenschutzbericht 1999 unter 4.1, S. 83) hatten die Datenschutzbeauftragten zahlreiche Änderungsvorschläge zu Detailanordnungen dieser bundeseinheitlichen Verwaltungsvorschriften unterbreitet. Erfreulicherweise wurden diese zum Teil berücksichtigt - wie etwa eine Unterrichtung auch über den errechneten Zeitpunkt des Ablaufs sowie der Wiederverleihung der Amtsfähigkeit, der Wählbarkeit oder des Wahl- und Stimmrechts bei Mitteilungen zum Wählerverzeichnis. Weitere Forderungen der Datenschutzbeauftragten, die der Justizministerkonferenz übermittelt wurden, sollten in den MiStra-Regelungen allerdings noch berücksichtigt werden, um dem Recht auf informationelle Selbstbestimmung Betroffener bei Mitteilungen in Strafverfahren in vollem Umfang Rechnung zu tragen. So fehlen insbesondere die Vorgaben einer ausschließlichen Anordnungsbefugnis von Staatsanwältinnen, Staatsanwälten, Richterinnen und Richtern sowie einer aus Transparenzgründen gebotenen **Benachrichtigung** Betroffener bei Übermittlung ihrer Daten.

17.1 Freiwillig in die DNA-Analyse-Datei?

Eine molekulargenetische Untersuchung von Körperzellen sowohl beschuldigter als auch verurteilter Personen zur Feststellung des DNA-Identifizierungsmusters zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren erfordert ebenso wie die vorangegangene Probenentnahme (etwa Mundspeichelabstriche) eine **richterliche Anordnung** (§ 81g Abs. 3 StPO, § 2 DNA-Identitätsfeststellungsgesetz i.V.m. § 81a Abs. 2 und § 81f StPO). Abweichend davon steht bei Gefährdung des Untersuchungserfolges durch Verzögerung nur die Anordnung der Probenentnahme auch der Staatsanwaltschaft und ihren Hilfsbeamtinnen und Hilfsbeamten zu. Bei der Anordnung ist unter anderem die **Prognose** zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten im Sinne des § 81g Abs. 1 StPO zu führen sind.

Problematisch ist, dass einzelne Gerichte (Landgericht Hamburg, Landgericht Berlin) richterliche Anordnungen in Fällen der **Einwilligung der Betroffenen** in die molekulargenetische Untersuchung als entbehrlich bezeichnet haben. Insbesondere bei Strafgefangenen kann jedoch nicht von einer Freiwilligkeit als Voraussetzung für eine rechtswirksame Einwilligung ausgegangen werden, könnten diese doch subjektiv Konsequenzen ihres Verhaltens für den weiteren Strafvollzug befürchten. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb bereits in ihrer Entschließung vom 7./8.10.1999 (siehe 15. Datenschutzbericht 2001, Anhang Nr. 9, S. 153/154) die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, als **unzulässige Umgehung** der gesetzlichen Regelung bezeichnet.

Diskutiert wird außerhalb Nordrhein-Westfalens auch, bei DNA-Analysen nach § 81g StPO, die mit Einwilligung der Betroffenen erfolgen, künftig nicht nur auf eine richterliche Anordnung, sondern - insoweit abweichend von der bisherigen Praxis - auch auf eine staatsanwaltschaftliche Negativprognose zu verzichten. Die Gefahrenprognose soll damit allein durch die Polizei erfolgen. Begründet wird die beabsichtigte Verfahrensänderung mit dem Hinweis darauf, dass die Beteiligung der Staatsanwaltschaft einen zusätzlichen Verwaltungsaufwand erfordere und angesichts der deutlichen Vorgaben des Bundesverfassungsgerichts für Negativprognosen entbehrlich sei. Es bedürfe einer Mitwirkung der Staatsanwaltschaft auch deshalb nicht,

weil die Betroffenen ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen könnten und eine entsprechende ausdrückliche Belehrung erfolge.

Diese Überlegungen stehen mit den **rechtlichen Anforderungen** nicht im Einklang. Die Feststellung, Speicherung und (künftige) Verwendung eines DNA-Identifizierungsmusters zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren greift nach der Rechtsprechung des Bundesverfassungsgerichts in das Recht auf informationelle Selbstbestimmung ein (BVerfG, Beschluss vom 15. März 2001, NJW 2001, S. 2320/2321). Dabei ist nach der Gesetzesbegründung die Prognoseentscheidung in Folge des **Richtervorbehalts** ebenfalls der Richterin oder dem Richter zugewiesen (BT-Drs. 13/10791, S. 5). Die Prognose setzt voraus, dass ihr eine zureichende Sachaufklärung vorausgegangen ist und die für sie bedeutsamen Umstände nachvollziehbar abgewogen werden. Sie muss eine auf den Einzelfall bezogene Entscheidung sein, *„die auf schlüssigen verwertbaren und in der Entscheidung nachvollziehbar dokumentierten Tatsachen beruht und die richterliche Annahme der Wahrscheinlichkeit künftiger Straftaten von erheblicher Bedeutung belegt."* (BVerfG aaO, S. 2320).

Es bedeutete also eine Abkehr von dem durch den Gesetzgeber angeordneten Richtervorbehalt, wenn auf eine richterliche Gefahrenprognose künftig in Fällen verzichtet würde, in denen eine - ohnehin rechtlich fragwürdige - Einwilligung der Betroffenen vorliegt. Die Anordnung des Richtervorbehalts darf nicht aus Praktikabilitätserwägungen unterlaufen werden. Das Justizministerium wurde auf die datenschutzrechtlichen Bedenken hingewiesen.

Aktuell hat das Landeskriminalamt den Kreispolizeibehörden „Hinweise zur DNA-Entnahme sowie zur DNA-Untersuchung und Datenverarbeitung im Rahmen der DNA-Analyse-Datei (DAD)" - Stand: Oktober 2002 - übersandt. Hierin wird betont, dass nach einvernehmlicher Auffassung des Justiz- und des Innenministeriums Körperzellen von Beschuldigten und Verurteilten grundsätzlich nur auf Anordnung der Ermittlungsrichterin oder des Ermittlungsrichters molekulargenetisch untersucht werden dürfen. Dies schließe aus, dass im Rahmen der polizeilichen Kriminalitätssachbearbeitung darauf hingewirkt werde, von Beschuldigten oder Verurteilten Einwilligungen in die molekulargenetische Untersuchung der Körperzellen und für die Speicherung des Untersuchungsergebnisses in der Datei zu verlangen. Das Landeskriminalamt vertritt unabhängig von der ministeriellen Vorgabe

dennoch die Auffassung, dass im Einzelfall eine molekulargenetische Untersuchung zum Zwecke der Speicherung in der Datei auf Grund einer Einwilligung Betroffener zulässig sei. Da allerdings in diesen Fällen die Einwilligung jederzeit mit der Folge widerrufen werden könne, dass die entsprechenden personenbezogenen Daten umgehend zu löschen seien, befürwortet es aus polizeilicher Sicht dennoch die nunmehr getroffene Regelung.

Diese Auffassung des Landeskriminalamtes zu den Modalitäten der Einstellung molekulargenetischer Untersuchungsergebnisse in die DNA-Analyse-Datei ist im Hinblick auf die verfassungsrechtlichen Vorgaben nicht haltbar. Die Datenspeicherung erfordert nach der Rechtsprechung des Bundesverfassungsgerichts in jedem Fall einen richterlichen Beschluss.

17.2 Muss eigentlich jeder Brief gelesen werden?

Wieder haben sich im Berichtszeitraum einige Strafgefangene wegen der Praxis bei der Kontrolle des Schriftverkehrs von Strafgefangenen in den Justizvollzugsanstalten beschwert.

Nach § 29 Strafvollzugsgesetz (StVollzG) dürfen bestimmte Schriftwechsel, beispielsweise die Verteidigerpost oder auch die Korrespondenz mit den Datenschutzbeauftragten des Bundes oder der Länder, nicht überwacht werden, sofern die Identität der Absenderin oder des Absenders zweifelsfrei feststeht. Der übrige Schriftverkehr darf überwacht werden, soweit es aus Gründen der Behandlung der oder des Gefangenen oder der Sicherheit oder Ordnung der Anstalt erforderlich ist und der Verhältnismäßigkeitsgrundsatz gewahrt wird. Das heißt, die Überwachung muss in einem angemessenen Verhältnis zu ihrem Zweck stehen und darf die Gefangenen nicht intensiver oder länger als notwendig beeinträchtigen. In einigen **Justizvollzugsanstalten** erfolgt jedoch, wie bereits im vorigen Berichtszeitraum festgestellt wurde, bei Kontrollen aus Gründen der Sicherheit unter Berufung auf § 29 Abs. 3 StVollzG unverändert eine **generelle Kontrolle des Schriftverkehrs** (siehe 15. Datenschutzbericht 2001 unter 6.2.1, S. 84/85). In der Praxis wird häufig wegen einzelner Strafgefangener, von denen eine Gefahr für die Sicherheit oder Ordnung der Justizvollzugsanstalt droht, auch der Briefverkehr aller anderen Strafgefangenen überwacht und damit in deren Grundrecht aus Art. 10 GG eingegriffen. Diese Problematik wurde in der Sitzung der Vollzugskommission des Rechtsausschusses des Landtags vom 25. April 2001 diskutiert, wobei darauf hingewiesen wurde, dass derartige Eingriffe in je-

dem Einzelfall gesondert am **Verhältnismäßigkeitsgrundsatz** zu messen sind.

In der weiteren Diskussion mit dem Justizministerium ist es gelungen, eine möglicherweise praxisgerechte Lösung zu finden. Es wurde vereinbart, dass die Justizvollzugsanstalten künftig regelmäßige Verfahrensprüfungen vornehmen und deren Ergebnisse schriftlich festhalten.

17.3 Erfassung von Besucherdaten

Mehrere Beschwerden betrafen die in einigen Justizvollzugsanstalten vorgenommene elektronische Erfassung von Besucherdaten.

Mittels Personalausweislesegeräten werden zur Führung der Besucherverzeichnisse - die früher handschriftlich in Büchern notiert wurden - auf Knopfdruck **Personalausweisdaten eingelesen**. Erfasst werden das Geburtsdatum, der Vor- und Zuname der Besucherin oder des Besuchers sowie die Gültigkeitsdauer des Ausweises. Weitere Daten (Wohnort, Name des oder der besuchten Strafgefangenen, Besuchszweck) werden manuell hinzugefügt. In einem folgenden Schritt werden die Daten gespeichert. Die Erhebung der Besucherdaten ist an sich grundsätzlich zulässig. Abzulehnen ist allerdings das **Verfahren**, personenbezogene Daten in Zusammenhang mit dem **automatischen Lesen des Personalausweises zu speichern**.

Im Gesetzgebungsverfahren zur Einführung des Personalausweises Mitte der 80er Jahre war zunächst höchst umstritten, ob dieser Ausweis überhaupt maschinenlesbar ausgestaltet sein sollte. Der Gesetzgeber ließ dies letztendlich zu, reduzierte aber die **Nutzung der Maschinenlesbarkeit** zur Speicherung der eingelesenen Daten für den öffentlichen Bereich in § 3a Abs. 2 des Personalausweisgesetzes (PAuswG) auf diejenigen Fälle, in denen die gleichzeitige Speicherung gesetzlich vorgeschrieben ist. Im privaten Bereich ist nach § 4 Abs. 3 PAuswG jegliche automatische Speicherung von aus dem Personalausweis eingelesenen Daten untersagt.

Diese gesetzgeberische Absicht wird nun durch die Lesegeräte in den Justizvollzugsanstalten, für die es an einer besonderen gesetzlichen Regelung fehlt, mit dem Hinweis unterlaufen, der Gesetzgeber hätte seinerzeit lediglich ein technisch gleichzeitig erfolgendes Einlesen und Speichern verhindern wollen. Demgegenüber würden den eingelesenen personenbezogenen Daten in den Justizvollzugsanstalten ergänzende Daten

hinzugefügt, bevor diese erst durch einen weiteren Befehl des oder der Bediensteten abgespeichert würden. Diese Lesart des Gesetzes verkennt, dass nicht die technische, auf Sekundenbruchteile exakte Gleichzeitigkeit von Lesen und Speichern entscheidend ist, sondern vielmehr der Umstand, dass die zum Identitätsnachweis im Personalausweis gespeicherten Daten letztlich zu **sachfremden Zwecken** - hier der Arbeitserleichterung der JVA-Beschäftigten - herangezogen werden. Gerade eine solche sachfremde Verwendung sollte aber durch die Einschränkung auf die ausdrücklich gesetzlich zugelassenen Fälle verhindert werden, und zwar nicht etwa, um den JVA-Beschäftigten oder anderen Stellen ihre Arbeit zu erschweren, sondern vielmehr, um weiteren Begehrlichkeiten und letztlich einem Missbrauch des Identitätspapiers einen Riegel vorzuschieben.

Eine Speicherung automatisch ausgelesener Personalausweisdaten zu gesetzlich nicht vorgesehenen Zwecken ist unzulässig. Leider konnte darüber bislang keine Einigung mit dem Justizministerium erzielt werden.

17.4 Elektronische Datenverarbeitung bei den Gerichten

Auch die Justiz geht mehr und mehr zum **Einsatz elektronischer Datenverarbeitung und automatisierter Verfahren** über. Abgesehen von solchen Programmen, die das Schreibwerk und die Verwaltungstätigkeit der Gerichte unterstützen, werden zunehmend auch die im Rahmen der freiwilligen Gerichtsbarkeit zu führenden Register wie **Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister** und nicht zuletzt auch das **Grundbuch** auf elektronische Führung umgestellt. Nach der Planung des Justizministeriums sollen etwa die bisher erst in Pilotprojekten eingerichteten Verfahren des elektronischen Grundbuchs bis Ende 2006 sowie das elektronische Handels- und Genossenschaftsregister - zunächst noch beschränkt auf Auskunftserteilung an Dritte - bis Ende 2003 landesweit eingeführt werden. In einem weiteren Schritt sollen zu einem bislang noch nicht festgelegten späteren Zeitpunkt auch Anmeldungen zu diesen Registern in elektronischer Weise zugelassen werden.

Aus datenschutzrechtlicher Sicht muss insbesondere die **Vertraulichkeit** und **Integrität** der Daten sichergestellt werden. Insoweit ist dafür Sorge zu tragen, dass nur **Befugte** auf die Daten zugreifen können und diese während der Verarbeitung unversehrt, vollständig und aktuell bleiben (§ 10 Abs. 2 DSG NRW).

Das im September 2002 vom Justizministerium eingerichtete **IT-Verfahren AUSCHU** (Automationsgestütztes Schuldnerverzeichnis) ermöglicht den Staatsanwaltschaften sowie weiteren Landesbehörden einen **lesenden Zugriff** auf die von den jeweiligen Amtsgerichten bei dem Gemeinsamen Gebietsrechnungszentrum Hagen geführten Schuldnerdateien durch automatisierten Abruf. Für die Umsetzung dieses - bundesweit ersten - automatisierten Schuldnerverzeichnisses fehlte es nach den Plänen des Justizministeriums zunächst an einer gemäß § 915h Abs. 2 Satz 1 ZPO erforderlichen Delegation der Verordnungsermächtigung von der Landesregierung an das Justizressort. Eine entsprechende Delegationsverordnung wurde sodann vorbereitet. In der Sache selbst wurde das Justizministerium in diesem frühen Stadium darauf hingewiesen, dass der Entwurf der zur Einrichtung des Verfahrens ermächtigenden Verordnung nicht erkennen ließ, wie sichergestellt sein sollte, dass nur **berechtigte Personen** innerhalb der jeweiligen Behörden **Zugriff** auf das zentrale **Schuldnerverzeichnis** haben, ein Zugriff nur **zur Erfüllung** der der jeweiligen Stelle obliegenden **Aufgaben** erfolgt und die gespeicherten Daten schließlich auch **nur in diesem Umfang zugänglich** gemacht werden. Außerdem war darauf hinzuweisen, dass in dem Entwurf keine **Protokollierungspflicht** vorgesehen war. Sie ist Voraussetzung für eine wirksame Kontrolle der Rechtmäßigkeit des jeweiligen Zugriffs auf die Daten des Schuldnerverzeichnisses. Nach der Stellungnahme des Justizministeriums wird insoweit sichergestellt, dass die Zugriffsmöglichkeit auf das zentrale Schuldnerverzeichnis ausschließlich auf den Bildschirmarbeitsplätzen der jeweiligen Bearbeiterinnen und Bearbeiter in den Vollstreckungs- und Erhebungsstellen zur Verfügung stehen soll. Neben dem Zugriff auf den durch ein persönliches Passwort zu sichernden PC selbst wird auch der Zugriff auf das zentrale Schuldnerverzeichnis bei dem Gemeinsamen Gebietsrechnungszentrum Hagen durch eine Benutzerauthentifizierung geschützt. Schließlich ist der lesende Zugriff nicht auf Datengruppen, sondern zur Wahrung eines dienstlichen Bezugs der Datenabfrage nur auf einzelne Datensätze möglich. Auch eine Protokollierungspflicht ist nunmehr vorgesehen. Mit diesen Maßnahmen lässt sich die Datensicherheit bei automatisierten Abrufen deutlich erhöhen.

Als erstes Bundesland veröffentlicht Nordrhein-Westfalen seit dem Frühjahr 2002 **Bekanntmachungen zu laufenden Insolvenzverfahren im Internet.** Außerdem finden sich dort bisweilen **elektronische Gerichtstafeln**, auf denen Versteigerungstermine in Zwangsversteigerungsverfahren bekannt gegeben werden. Das hat den Vorteil, dass gerade die Zwangsversteigerungstermine einem größeren Publikum bekannt gemacht werden können.

was nicht zuletzt zu einem höheren Versteigerungserlös führen und damit den Betroffenen zugute kommen kann. Die damit leider ebenfalls verbundenen **Nachteile** liegen jedoch auf der Hand: Selbst wenn diese Informationen nach Ablauf bestimmter Fristen von der virtuellen Gerichtstafel wieder entfernt worden sind, bedeutet dies keineswegs, dass die personenbezogenen Daten, etwa der Name der (gegebenenfalls auf Grund der bekannt gegebenen Anschrift ermittelbaren) Eigentümerinnen und Eigentümer der zu versteigernden Objekte, damit aus dem world wide web verschwunden wären. Verlage, Auskunfteien und Wirtschaftsinformationsdienste können die Daten vielmehr nutzen, um eigene Verzeichnisse „nicht kreditwürdiger Personen" zu erstellen. Mit Hilfe von Suchmaschinen können die Betroffenen so noch nach Jahren mit ihren früheren finanziellen, möglicherweise längst behobenen Schwierigkeiten in Verbindung gebracht werden - sozusagen in ewigem Andenken an die Pleite.

Für den Bereich des Insolvenzrechts, das gerade auch die Möglichkeit der Restschuldbefreiung vorsieht, hat der Bundesgesetzgeber die Schädlichkeit solcher „**Altdaten im Internet**" erkannt und im Verordnungsweg sowohl Fristen, nach deren Ablauf eine **Abfrage** nur noch unter Angabe bestimmter Details zu dem Verfahren (Sitz des Insolvenzgerichts und mindestens eine der weiteren Angaben: Familienname, Firma, Sitz oder Wohnsitz der Schuldnerin oder des Schuldners oder Aktenzeichen des Insolvenzgerichts) möglich ist, als auch **Löschungsfristen** eingeführt. Der Bundesdatenschutzbeauftragte hat sich in Abstimmung mit den Datenschutzbeauftragten der Länder des Weiteren an die Bundesministerien für Justiz und Inneres gewandt und gefordert, durch eine Änderung des Bundesdatenschutzgesetzes die **Veröffentlichung** von Informationen, die von einem Gericht nur temporär in das Internet eingestellt werden dürfen, nach Ablauf der dafür vorgesehenen Fristen auch für **Dritte generell zu untersagen**. Während dieser Vorschlag bereits positiv aufgenommen wurde, ist allerdings die weitergehende Forderung, Dritten auch eine Internet-Veröffentlichung von Daten aus amtlichen Bekanntmachungen in schriftlicher Form nach Ablauf der für das Gericht bestimmten Veröffentlichungs- oder Löschungsfristen zu untersagen, bislang nicht auf Gehör gestoßen. Allerdings haben sich inzwischen mehrere Bürgerinnen und Bürger über eine **Stigmatisierung durch fortdauernde Internet-Veröffentlichung ihrer Insolvenz- oder Zwangsversteigerungsdaten** beschwert. Das Justizministerium wurde gebeten, das Datenschutzanliegen im Bundesrat zu unterstützen. Es hat inzwischen versichert, dass auf der entsprechenden Homepage des Landes (www.zvg.nrw.de) die Namen der

jeweiligen Eigentümerinnen und Eigentümer nicht genannt werden. Die Problematik ist damit teilweise entschärft.

18 Rechtsanwältinnen und Rechtsanwälte

Einige Rechtsanwältinnen und Rechtsanwälte, die im Rahmen der Bearbeitung von Bürgereingaben um Auskunft und Stellungnahme gebeten wurden, lehnten das Ersuchen mit Hinweis auf die gegenüber ihrer Mandantschaft bestehende Verschwiegenheitspflicht ab. Sie waren der Ansicht, dass ihnen aufgrund der Strafbarkeit einer Verletzung dieser Pflicht (§ 203 Abs. 1 Nr. 3 Strafgesetzbuch (StGB)) ein Auskunftsverweigerungsrecht nach § 38 Abs. 3 Satz 2 BDSG zustünde.

Dass dies nicht so ist, ergibt sich aus den Vorschriften des BDSG: Gemäß § 38 Abs. 3 Satz 1 BDSG sind alle der Datenschutzkontrolle unterliegenden Stellen **zur Auskunft verpflichtet.** Nach Satz 2 der Vorschrift kann die Auskunft nur auf solche Fragen verweigert werden, deren Beantwortung den Auskunftspflichtigen selbst oder bestimmte Angehörige der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Aus dieser Formulierung („...solche Fragen, ... deren Beantwortung...") folgt, dass eine Auskunftsverweigerung nur dann in Betracht kommt, wenn sich die Strafbarkeit der Rechtsanwältin oder des Rechtsanwalts inhaltlich aus dem Sachverhalt, über den Auskunft erteilt wird, ergeben könnte. Damit begründet nicht die mit der Auskunft selbst verbundene Offenlegung von Details aus dem Mandantenverhältnis ein Auskunftsverweigerungsrecht. Ein solches besteht vielmehr nur dann, wenn mit der Auskunft ein Lebenssachverhalt preisgegeben würde, aus dem sich die Begehung einer Straftat oder Ordnungswidrigkeit ergibt.

Gestützt wird dieses Ergebnis durch §§ 24 Abs. 2 Satz 1 Nr. 2 i.V.m. Abs. 6, 38 Abs. 4 Satz 3 BDSG. Danach erstreckt sich die **datenschutzrechtliche Kontrolle** im Rahmen von Prüfungen und Besichtigungen vor Ort auch auf personenbezogene Daten, die einem **Berufsgeheimnis** unterliegen. Für die im vorgehenden Absatz (§ 38 Abs. 3 BDSG) geregelte Pflicht zur Auskunftserteilung kann nichts anderes gelten. Denn andernfalls wäre die Aufsichtsbehörde bei Rechtsanwältinnen und Rechtsanwälten, die sich nicht kooperativ verhalten, stets auf Prüfungen und Besichtigungen vor Ort angewiesen, um diesen gegenüber ihrer gesetzlichen Kontrollaufgabe gerecht zu werden.

Angesichts dieser grundsätzlichen Auskunftspflicht, die gerade eine Befugnis zur Datenübermittlung gewährt, handeln Rechtsanwältinnen und Rechtsanwälte, die gegenüber der Aufsichtsbehörde dem Berufsgeheimnis

unterliegende Daten offenbaren, nicht „unbefugt" im Sinne des § 203 Abs. 1 StGB. Da sie sich somit nicht der Gefahr strafgerichtlicher Verfolgung aussetzen, besteht kein Auskunftsverweigerungsrecht unter Berufung auf die anwaltliche Verschwiegenheitspflicht.

Auch Rechtsanwältinnen und Rechtsanwälte sind daher gegenüber der Landesbeauftragten für den Datenschutz grundsätzlich zur Auskunft verpflichtet.

19 Finanzen

19.1 Information über Daten zur eigenen Person

Selbst in Zeiten der Informationsfreiheit sind immer noch die alten Widerstände gegen das in § 18 DSG NRW verankerte Recht der Steuerpflichtigen auf Einsichtnahme in die Steuerakte zu ihrer *eigenen* Person nicht beseitigt.

Unter Hinweis auf den so genannten Anwendungserlass des Bundesministeriums der Finanzen vom 15. Juli 1998 - IV A 4 - S 0062 - 13/98 - zur Abgabenordnung 1977 - hier: Nr. 4 zu § 91 Abgabenordnung (AO) - vertreten die Finanzbehörden leider immer noch die Auffassung, die Entscheidung über **Akteneinsicht** und **Auskunftserteilung** in oder aus Steuerakten liege im Ermessen der Finanzbehörden. In nicht nachvollziehbarer Weise wird eine bloße Verwaltungsvorschrift über das Gesetz gestellt. Dies wird damit begründet, dass die AO keine Regelung zur Akteneinsicht enthalte und damit ein Akteneinsichtsrecht der Steuerpflichtigen im Besteuerungsverfahren nicht gewollt sei.

Es wird weiterhin negiert, dass die Steuerpflichtigen nach § 18 DSG NRW **auch im Steuerbereich** grundsätzlich ein anlassunabhängiges Akteneinsichts- und Auskunftsrecht gegenüber den Finanzbehörden haben. Eine diese datenschutzrechtliche Grundregel einschränkende Bestimmung im Sinne des § 2 Abs. 3 DSG NRW gibt es in der Abgabenordnung nicht. Den - von der Finanzverwaltung gegen das Akteneinsichtsrecht immer wieder ins Feld geführten - Ermittlungsinteressen der Steuerbehörden sowie den Datenschutzinteressen Dritter wird durch § 18 Abs. 3 DSG NRW in ausreichendem Umfang Rechnung getragen. Erstaunlicherweise wird häufig **ausgerechnet das Steuergeheimnis** den betroffenen Steuerpflichtigen zur Begründung einer Ablehnung ihres nach § 18 DSG NRW bestehenden Akteneinsichtsrechtes entgegen gehalten. Es ist offenbar immer noch nicht verstanden worden, dass das Steuergeheimnis Teil des Datenschutzes ist.

Solange es keine anderslautende Regelung des Akteneinsichtsrechts in der AO gibt, muss jede generelle Verweigerung der Akteneinsicht gegenüber Steuerpflichtigen als Verstoß gegen den Datenschutz beanstandet werden.

19.2 Durchsuchungen bei Dritten

In steuerstrafrechtlichen Ermittlungsverfahren gelten Beschuldigte bis zu einer etwaigen rechtskräftigen Verurteilung als unschuldig. Sie haben Anspruch darauf, dass ihre grundgesetzlich geschützten Persönlichkeitsrechte bei jeder Maßnahme der Steuerfahndung angemessen berücksichtigt werden.

In einem vom Finanzamt für Steuerstrafsachen und Steuerfahndung betriebenen Verfahren musste folgendes Defizit grundsätzlicher Art festgestellt werden: Im Zuge von Ermittlungen gegen einen Beschuldigten war ein gerichtlicher **Durchsuchungsbeschluss** gegen eine andere Person als den Beschuldigten (§§ 103 ff. 162 Strafprozessordnung) erwirkt worden. Der Beschluss war selbstverständlich der von der Durchsuchung betroffenen Person bekannt zu geben. Damit erhielt sie aber auch Kenntnis unter anderem von Namen und Anschrift des Beschuldigten sowie dem steuerrechtlichen Tatvorwurf. Mit der Bekanntgabe des Durchsuchungsbeschlusses kann also eine Bloßstellung bewirkt werden, die beispielsweise für Inhaberinnen und Inhaber eines Gewerbebetriebes weitreichende Folgen haben kann. Die Situation kann sich insbesondere verschlimmern, wenn die Daten aus dem Durchsuchungsbeschluss an unbeteiligte Personen weitergegeben werden. Der Personenkreis, dem gegenüber sich der Beschuldigte an den **Pranger** gestellt sieht, ist nicht eingrenzbar, weil das normalerweise schützende Steuergeheimnis die Person, die Kenntnis aus dem Durchsuchungsbefehl erlangt hat, nicht mehr erfasst und zur Geheimhaltung verpflichtet. Umso mehr muss die Durchführung einer steuerstrafrechtlichen Ermittlung im Einklang mit den rechtsstaatlichen Verfahrensgrundsätzen stehen. Darauf hat das Finanzministerium selber in seinen „Anweisungen für das Straf- und Bußgeldverfahren (Steuer)" vom 20. Juni 1995 hingewiesen. Zur Einhaltung rechtsstaatlicher Verfahrensgrundsätze gehört auch die **Einhaltung** von Vorschriften über den **Datenschutz**, insbesondere des § 16 Abs. 2 DSG NRW. Deshalb ist die Empfängerin oder der Empfänger von Daten Dritter darauf **hinzuweisen**, dass die Daten aus dem Durchsuchungsbeschluss nur zum Zwecke der Überprüfung der Rechtmäßigkeit der Durchsuchung genutzt und nicht an andere übermittelt werden dürfen.

Dem würde die Finanzbehörde Rechnung tragen, wenn sie mit dem Durchsuchungsbeschluss eine besondere **schriftliche Belehrung** über dieses

Übermittlungsverbot an die von der Durchsuchung betroffene Person aushändigt. Die Belehrung sollte auch den Hinweis darauf enthalten, dass ein Verstoß gegen das Verbot mit einem Bußgeld geahndet werden kann.

Bedauerlicherweise sieht das Finanzministerium NRW keine Notwendigkeit, diese Anregung aufzugreifen und die bereits bestehenden Anweisungen zum Ablauf einer Durchsuchung entsprechend zu ergänzen. Es verweist darauf, dass die Steuerfahndungsstellen bei der Beantragung von Durchsuchungsbeschlüssen gegen Dritte stets nur die unbedingt erforderlichen personenbezogenen Daten an die zuständigen Stellen übermitteln würden. Da diese Argumentation an der Problematik vorbeigeht, wurde das Finanzministerium auf die datenschutzrechtlichen Bedenken einer möglichen zweckfremden Nutzung der Daten durch Dritte hingewiesen und gebeten, seine Haltung noch einmal zu überdenken. Durch eine einfache **Ergänzung von Verwaltungsvorschriften** könnte der Datenschutz verbessert werden, und zwar ohne die Aufgabenerfüllung der Finanzbehörden für Steuerstrafsachen und -fahndung zu beeinträchtigen.

Mit dem Durchsuchungsbeschluss sollte auch eine schriftliche Belehrung darüber ausgehändigt werden, dass die im Beschluss genannten personenbezogenen Daten nicht an unbeteiligte Personen übermittelt werden dürfen.

20 Statistik

20.1 Zensustestgesetz

Die Bemühungen, künftig im Rahmen einer Volkszählung auf eine teure flächendeckende Befragung der Bevölkerung verzichten zu können, sind mit dem In-Kraft-Treten des Gesetzes zur Erprobung eines registergestützten Zensus (Zensustestgesetz - ZensTeG) vom 27. Juli 2001 ein gutes Stück vorangekommen. Während im Berichtszeitraum des 15. Datenschutzberichts 2001 erst ein Entwurf des Testgesetzes vorlag, hat das Landesamt für Datenverarbeitung und Statistik des Landes Nordrhein-Westfalen (LDS NRW) die wesentlichen Vorarbeiten für den Test zwischenzeitlich abgeschlossen und seit Ende November 2001 mit der Durchführung begonnen. Im Einzelnen ordnet das Zensustestgesetz als **Bundesstatistik** verschiedene Testerhebungen, Untersuchungen von Registern und statistisch-methodische Untersuchungen an.

Nach den Bemühungen, eine **datenschutzkonforme Gestaltung** des Gesetzes zu erreichen (vgl. insoweit die Ausführungen im 15. Datenschutzbericht 2001 unter 14., S. 122), galt es nunmehr sicherzustellen, dass auch bei der **Umsetzung** des Gesetzes und der weiteren Datenverarbeitung den Erfordernissen des Datenschutzes bei statistischen Erhebungen entsprochen wird. Veranlassung hierzu gab im Berichtszeitraum ein vom Statistischen Bundesamt entworfener „Fragebogen zum Hauptwohnsitz" im Rahmen der Befragung betroffener Einwohner und Einwohnerinnen nach § 3 Abs. 3 ZensTeG. Bei dieser Erhebung unterliegen die Betroffenen gemäß § 13 Abs. 3 ZensTeG einer **Auskunftspflicht**. Der Entwurf des Fragebogens enthielt zunächst lediglich die Formulierung: „Wir bitten Sie, die Fragen im Erhebungsbogen zu beantworten....". Eine solche Formulierung macht den zu Befragenden nicht deutlich, ob sie zur Auskunft verpflichtet sind oder ob es ihnen freisteht, die gewünschten Auskünfte zu erteilen. Das Problem wurde inzwischen durch die Aufnahme eines eindeutigen Hinweises auf die Auskunftspflicht beseitigt.

Problematisch dürfte auch die vorgesehene Klärung der Mehrfachfälle sein. Mehrfachfälle sind dabei **mehrere Anschriften** in einer oder mehreren Gemeinden, auch wenn nur **teilidentische Personalien** zu diesen Anschriften vorliegen. Wenn im Fragebogen hierfür auch Anschriften zu einer Person aufgelistet werden, die tatsächlich zu einer anderen Person gehören, dürfte diese Vorgehensweise der Datenübermittlung an Dritte

gegen das **Statistikgeheimnis** verstoßen. Die vom Statistischen Bundesamt angenommene „sehr hohe Wahrscheinlichkeit" einer Personenidentität reicht hier nicht aus.

Das Zensustestgesetz dient zunächst nur dazu, die registergestützten neuen Verfahren zur Datengewinnung im Hinblick auf eine spätere Volkszählung eingehend zu erproben. Zensusdaten werden ausschließlich zu diesem Zweck erhoben. Eine beliebige Weitergabe oder Nutzung durch einzelne Ämter ist mithin nicht möglich. Rückmeldungen von den statistischen Ämtern an die registerführenden Verwaltungsbehörden sind zudem nicht zulässig.

Erste Ergebnisse des Zensustests sollen im Jahr 2003 vorliegen. Insofern bleibt abzuwarten, ob der Test der neuen Methode erfolgreich verläuft und die grundlegenden Erfordernisse des Datenschutzes, die bei statistischen Erhebungen gelten, auch bei Umsetzung der Ergebnisse und Methoden in ein neues Gesetz Beachtung finden.

20.2 Zählung des Verkehrsaufkommens

Eine größere Stadt in Nordrhein-Westfalen beabsichtigte zur Fortschreibung der Verkehrsentwicklungs- und Nahverkehrsplanung eine umfangreiche Ermittlung von Grundlagendaten zum Verkehrsaufkommen und -geschehen in der Stadt durchzuführen. Den Auftrag zur Vorbereitung, Durchführung, Auswertung und Dokumentation der Untersuchung erhielt ein Ingenieurbüro. Das Vorhaben wurde zur datenschutzrechtlichen Prüfung vorgelegt.

Die Zählung des Verkehrsaufkommens bestand aus den drei Bausteinen Erhebung der Mobilität der Bevölkerung, des Pendlerverkehrs und des Wirtschaftsverkehrs. Obwohl Ziel der Erhebung lediglich die Gewinnung (anonymer) **statistischer Daten** war, wurden - bedingt durch das Verfahren, die inhaltliche Gestaltung der Fragebogen und die Gewinnung der Adressdaten für die Befragung - zunächst tatsächlich durchweg auch **personenbezogene Daten erhoben** und verarbeitet. Zur Wahrung des Rechts auf informationelle Selbstbestimmung der Betroffenen mussten deshalb **Schutzvorkehrungen** durch Änderung des Verfahrens und der eingesetzten Fragebogen bis hin zur Änderung des Verfahrens der Auswertung vorgenommen werden, wie die folgenden Beispiele zeigen:

- So wurden die Erhebungsunterlagen für die Haushaltsbefragung und die Betriebsbefragung nicht mehr persönlich vom Hilfspersonal des Ingenieurbüros verteilt und abgeholt. Die Unterlagen der Haushaltsbefragung wurden vielmehr von der **Stadt selbst verschickt**. Dadurch wurde vermieden, dass das Ingenieurbüro als Stelle des Privatrechts von der Stadt Adressdaten von Bürgerinnen und Bürgern erhält und speichert, die eine Teilnahme an der Befragung ablehnen.
- Die Adressdaten der Betriebe wurden vom Ingenieurbüro aus **allgemein zugänglichen Quellen** entnommen und ebenfalls verschickt.
- Zur Wahrung der Datenschutzrechte Drittbetroffener, die nicht verpflichtet sind, ihre Daten den jeweils angeschriebenen Personen gegenüber zu offenbaren, wurde sichergestellt, dass diese ihre Angaben **direkt gegenüber dem Ingenieurbüro** machen können.
- Die Adressangaben wurden bei Eingang der ausgefüllten Fragebogen **verschlüsselt** und die Originalerhebungsbogen **vernichtet**. Damit war die **Anonymität** der Befragten von diesem Zeitpunkt an auf Dauer gewährleistet.

Insgesamt ist es bei diesem Vorhaben gelungen, dass die den Bürgerinnen und Bürgern gegenüber verwendeten Begriffe bei dieser Befragung wie beispielsweise „Einwilligung", „Freiwilligkeit", „Anonymität" nicht nur als (inhaltsleere) Etikette dienten, sondern jeweils eine konkrete Umsetzung des Rechts auf informationelle Selbstbestimmung der Betroffenen darstellten. Trotz des großen Kreises der teilnehmenden Personen sind - bezogen auf die jeweiligen einzelnen Befragungsfälle - keine Beschwerden mehr bekannt geworden.

21 Behördliche und betriebliche Datenschutzbeauftragte

21.1 Datenschutzbeauftragte bei öffentlichen Stellen

Mit der Änderung des Datenschutzgesetzes Nordrhein-Westfalen Mitte 2000 wurden alle Behörden und sonstigen öffentlichen Stellen im Lande durch § 32a DSG NRW verpflichtet, behördliche Datenschutzbeauftragte zu bestellen.

Diese gesetzliche Vorgabe ist in einigen Bereichen nur sehr zögerlich umgesetzt worden. Vielfach bestanden in den Behörden auch Fragen zur Interpretation des § 32a DSG NRW. Die dringlichsten Fragen wurden deshalb in der an Datenschutzbeauftragte und Behördenleitungen gerichteten **Orientierungshilfe „Behördliche Datenschutzbeauftragte"** aufgegriffen und beantwortet, die seit Frühjahr 2001 erhältlich ist.

Auch nach Veröffentlichung der Broschüre war im Einzelfall wiederholt zu klären, unter welchen Voraussetzungen **mehrere Stellen eine gemeinsame Datenschutzbeauftragte oder einen gemeinsamen Datenschutzbeauftragten** bestellen können. In allen Fällen konnten für die betroffenen Stellen geeignete Lösungen gefunden werden, die auch ein angemessenes Datenschutzniveau in den Behörden gewährleisten.

Die Frage nach der Zulässigkeit der Bestellung externer Berater galt es im **Hochschulbereich** zu klären. Hier hatten Privatunternehmen, die die Dienstleistungen einer oder eines betrieblichen Datenschutzbeauftragten nach dem BDSG für die nicht-öffentlichen Stellen anbieten, auch einzelne Hochschulen angesprochen. Es konnte einvernehmlich mit dem Wissenschaftsministerium geklärt werden, dass das DSG NRW anders als das BDSG die Bestellung **externer Datenschutzbeauftragter nicht zulässt**. Es kommt nach dem DSG NRW wesentlich darauf an, dass die oder der Datenschutzbeauftragte auch Kenntnisse über die internen Abläufe der öffentlichen Stelle hat. Das DSG NRW verlangt deshalb ausdrücklich die Bestellung interner Datenschutzbeauftragter. Unabhängig von der Bestellung der oder des Datenschutzbeauftragten kann sich eine öffentliche Stelle natürlich in Datenschutzfragen **zusätzliche Beratung** durch externe Fachleute einholen. Sie wird dabei darauf zu achten haben, dass solchen externen Fachleuten nur dann personenbezogene Daten zur Kenntnis gegeben werden, wenn dies für deren Aufgabenstellung erforderlich ist. Bei einer erforderlichen Weitergabe von personenbezogenen Daten an eine

Fachberaterin oder einen Fachberater sind die Regelungen über die **Datenverarbeitung im Auftrag** einzuhalten.

Für die behördlichen Datenschutzbeauftragten bestand eines der dringlichsten Probleme darin, eine **Definition des im DSG NRW verwendeten Begriffs „Verfahren"** zu erhalten. Die behördlichen Datenschutzbeauftragten haben mit der Novelle des DSG NRW im Jahr 2000 die Aufgabe erhalten, ein **Verfahrensverzeichnis** (§ 8 DSG NRW) zu führen, das sie zur Einsicht für alle interessierten Personen vorhalten. Zudem müssen sie bei Einführung neuer Verfahren ebenso wie bei einer wesentlichen Änderung laufender Verfahren gemäß § 10 Abs. 3 i.V.m. § 32a Abs. 1 Satz 7 DSG NRW eine **Vorabkontrolle** durchführen. Um diese Aufgaben zu bewältigen, müssen die Datenschutzbeauftragten eine Vorstellung davon entwickeln, was aus der Gesamtheit der automatisierten Datenverarbeitung als einzelnes Verfahren im Sinne dieser Vorschriften begriffen werden kann. Vor derselben Fragestellung stehen auch die Verantwortlichen in den Behörden, die **Sicherheitskonzepte** gemäß § 10 DSG NRW für automatisierte Verfahren erstellen müssen.

Folgende Erläuterung kann zum **Verfahrensbegriff** gegeben werden:

Die Regelungen zum Verfahrensverzeichnis und zur Vorabkontrolle haben ihre Wurzeln in der EG-Datenschutzrichtlinie. Nach Artikel 18 der Richtlinie unterliegt eine

- automatisierte Verarbeitung personenbezogener Daten

  oder eine

- Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrere verbundener Zweckbestimmungen

der Meldepflicht. Die Meldepflicht kann sich danach auf jede einzelne automatisierte Verarbeitung personenbezogener Daten beziehen. Anknüpfungspunkt kann aber auch ein so genanntes Bündel von Verarbeitungen sein.

Werden die beiden Möglichkeiten zugrunde gelegt, die die Richtlinie als Anknüpfungspunkt für die Meldepflicht eröffnet, wird deutlich, dass das DSG NRW die zweite Alternative aufgreift, denn ein **Verfahren** beschränkt sich - nach dem allgemeinen Verständnis von diesem Begriff - nicht auf einen einzelnen Verarbeitungsschritt, sondern stellt einen **Ablauf von Verarbeitungsschritten** dar. Die Begründung zur EG-Datenschutzrichtlinie

bietet für die oben angegebene „Mehrzahl von Verarbeitungen" eine Definition, die für das Verfahren übernommen werden kann. Danach ist ein Verfahren ein Paket der repetitiven (wiederholenden) oder nichtrepetitiven Verarbeitungen, mit denen eine oder mehrere vom Standpunkt der für die Verarbeitung verantwortlichen Person und der betroffenen Person aus miteinander verbundene Zweckbestimmung(en) realisiert werden soll(en).

Diese Definition geht zunächst von der **Zweckbestimmung** der Datenverarbeitung aus, wie sie sich nach der Vorstellung der für die Datenverarbeitung verantwortlichen Person darstellt. Um ein Verfahrensverzeichnis zu erstellen, wäre danach der erste Schritt die Überlegung, für welche Zwecke die Behörde Daten verarbeitet. Dabei können mehrere Zwecke in einem Verfahren verbunden sein. So kann beispielsweise ein automatisierter Datenverarbeitungszweck „Personalverwaltung" sein. Im entsprechenden Verfahren zur Personalverwaltung sind unter anderem alle Soft- und Hardwarekomponenten zu beschreiben (§ 8 Nr. 8 DSG NRW) - so zum Beispiel auch Word, Access oder Excel, wenn diese Programme für den Zweck „Personalverwaltung" eingesetzt werden. Daneben gibt es möglicherweise ein Verfahren „Gleitzeiterfassung" oder ein Verfahren „Beihilfensachbearbeitung", das dann jeweils entsprechend in der Verfahrensbeschreibung darzustellen ist.

Die datenverarbeitende Stelle kann den Zweck der Datenverarbeitung natürlich anders definieren, wenn ihr das praktikabel erscheint. So kann sie etwa die „Personalverwaltung - Beamte" und „Personalverwaltung - Angestellte" auch als eigenständige Zwecke formulieren, wenn dies sinnvoll ist, weil diese Teilverarbeitungen mit sehr unterschiedlichen Softwarekomponenten erfolgen. Gegebenenfalls kann neben dem Verfahren „Personalverwaltung" ein eigenständiges Verfahren „Fortbildungsmanagement" betrieben werden, weil diese Verfahren isoliert voneinander betrachtet und übersichtlicher dargestellt werden können. Es hängt von der **Organisation** in der datenverarbeitenden Stelle ab, welche **Datenverarbeitungszwecke** als eine abgeschlossene **Einheit** betrachtet werden können und zu einem Bündel zusammengefasst werden können, das ein in sich abgeschlossenes Verfahren darstellt.

Es empfiehlt sich nicht, an eine Zweckbestimmung anzuknüpfen, die etwa eine Beschreibung einzelner Word, Excel- oder Accessdateien erfordern würde. Eine zu **kleinteilige Verfahrensbeschreibung** hat den Nachteil, dass

sie nicht den **Überblick** verschaffen kann, der dem Sinn des Verfahrensverzeichnisses entspricht.

Die Zweckbestimmungen sollten außerdem so gewählt werden und miteinander verbunden sein, dass die von der Datenverarbeitung betroffenen Personen sie **nachvollziehen können**. Die Mitarbeiterin oder der Mitarbeiter soll erkennen können, dass ihre oder seine Daten im Verfahren „Personalverwaltung" verarbeitet werden. Wohingegen die Personen, die etwa mit dem Ausländeramt einer Kommune Kontakt haben, ihre Daten in anderen Verfahren suchen werden. Als Korrektiv für von der verantwortlichen Stelle gewählte Zweckbestimmungen, die ein Verfahren beschreiben, dient also immer die Frage: Lässt sich unter dem gewählten Zweck für die Betroffenen noch erkennen, dass in diesem Verfahren ihre Daten verarbeitet werden? Würde beispielsweise eine Kommune ein einziges Verfahren unter dem Gesamtzweck „Kommunalverwaltung" definieren und alle Datenverarbeitungen der Behörde darstellen, wäre dieses Bündel von Datenverarbeitungen **zu grob geschnürt**. Diese Zweckbestimmung hätte für die von der Datenverarbeitung Betroffenen **keine Aussagekraft** mehr. Das Einsichtsrecht gemäß § 8 Abs. 2 DSG NRW würde dann leer laufen.

Insgesamt ist festzustellen, dass die Bestellung von behördlichen Datenschutzbeauftragten und das gesetzliche Erfordernis zur Erstellung von Verfahrensverzeichnissen und zur Durchführung von Vorabkontrollen zu einer **größeren Sensibilisierung** vor Ort für die Belange des Datenschutzes geführt hat. Dies ging einher mit einer deutlichen Zunahme von Beratungsersuchen von Datenschutzbeauftragten und auch von Verantwortlichen in den Behörden.

Es ist deshalb ein wichtiges Ziel, die durch Einzelanfragen bekannt gewordenen Probleme aufzubereiten und Informationen zum Datenschutz für alle Behörden und behördlichen Datenschutzbeauftragten vorzuhalten. Um diese Informationsaufbereitung bedarfsgerecht auszurichten, wurde eine Umfrage zur Situation der behördlichen Datenschutzbeauftragten bei einem Teil der Behörden im Lande begonnen.

21.2 Betriebliche Datenschutzbeauftragte

Wie können Verstöße gegen die Datenschutzgesetze von vornherein verhindert werden? Indem der Datenschutz in den Unternehmen durch Informationen und Beratung gefördert wird, um Verletzungen des Rechts auf informationelle Selbstbestimmung vorzubeugen. Genau das ist Ziel der regelmäßigen Besprechungen mit den Datenschutzbeauftragten nordrhein-westfälischer Konzerne.

Kurz nachdem die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich übernommen wurde, wurden im Jahr 2000 erstmals die Datenschutzbeauftragten verschiedener nordrhein-westfälischer Konzerne zu einer Besprechung eingeladen. Seitdem trifft sich eine stetig wachsende Zahl von Teilnehmerinnen und Teilnehmern halbjährlich mit der Aufsichtsbehörde zum **Erfahrungs- und Informationsaustausch**. Um unternehmensspezifische Problemfelder besser kennen zu lernen und die datenschutzrechtliche Zusammenarbeit mit den jeweils Verantwortlichen zu intensivieren, werden über die halbjährlichen Besprechungen hinaus auch **Informationsbesuche** bei größeren Unternehmen und Konzernen des Landes durchgeführt. Insgesamt betrachtet ist der regelmäßige Informations- und Erfahrungsaustausch sowie die dadurch verbesserte Kooperation mit den betrieblichen Datenschutzbeauftragten ein Erfolg versprechender Schritt auf dem Weg zum vorsorgenden Datenschutz.

Auch wenn es nicht möglich ist, sich mit den Datenschutzbeauftragten aller in Nordrhein-Westfalen ansässigen Unternehmen zu treffen, so handelt es sich bei der Besprechung der Konzerndatenschutzbeauftragten doch um eine offene Runde, zu der alle interessierten Datenschutzbeauftragten großer Unternehmen oder Konzerne herzlich willkommen sind.

22 Das neue Informationsfreiheitsgesetz

Das neue Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) verfolgt den Zweck, den **freien Zugang** zu den bei den öffentlichen Stellen vorhandenen Informationen zu gewährleisten und die grundlegenden Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden sollen (§ 1 IFG NRW). Jede natürliche Person hat nunmehr nach Maßgabe dieses Gesetzes grundsätzlich einen **Anspruch** auf Informationszugang und damit auf Teilhabe an den bei öffentlichen Stellen vorhandenen amtlichen Informationen. Damit sollen den Informationssuchenden Verwaltungsentscheidungen transparent gemacht und auch eine Kontrolle des Verwaltungshandelns ermöglicht werden. In der täglichen Verwaltungspraxis muss der Wechsel vom Amtsgeheimnis zur **Aktenöffentlichkeit** allerdings erst nachvollzogen werden.

22.1 Zur „Sicherstellung" des Rechts auf Information

Das IFG NRW hat im Vergleich zu anderen neuen Gesetzen schon mit In-Kraft-Treten eine große Resonanz sowohl bei den Bürgerinnen und Bürgern als auch bei den öffentlichen Stellen hervorgerufen. Auf Seiten der Informationssuchenden dominiert ein großes Nachholbedürfnis, endlich den manchmal schon vergeblich erstrebten Zugang zu Informationen bei der öffentlichen Verwaltung zu erreichen. Demgegenüber sind auf Seiten der Verwaltung zurückhaltende oder sogar vorsichtig abwehrende Reaktionen auf die gestellten Anträge zu verzeichnen.

Im ersten Jahr gingen hier bereits zahlreiche schriftliche und telefonische **Beschwerden** der Informationssuchenden und **Anfragen** aus der Verwaltung ein. Viele Fälle konnten erst nach wiederholtem Schriftverkehr mit den öffentlichen Stellen erledigt werden, denn bei der Mehrzahl der zu Unrecht abgelehnten Anträge bedurfte es einiger Überzeugungsarbeit, bevor die Verwaltungen bereit waren, den beantragten Informationszugang zu gewähren. Oft spielten dabei Erwägungen eine Rolle, die dem erklärten Willen des Gesetzgebers zuwider liefen.

Überwiegend stammten die Anfragen und Beschwerden von Bürgerinnen und Bürgern, die Informationen im eigenen Interesse erlangen wollten. Daneben fragten aber auch viele Initiativen, Vereine und

Interessengemeinschaften sowie Gesellschaften und Unternehmen an, warum ihre Anträge - oft bereits aus „formalen Gründen" - abgelehnt worden seien; sie waren dabei manchmal noch nicht einmal darauf hingewiesen worden, dass nach Maßgabe des IFG NRW nur eine **natürliche Person** einen Anspruch auf Informationszugang geltend machen kann. Es erscheint - auch im Hinblick auf die europäische Entwicklung des Informationszugangsrechtes - sinnvoll, die „künstliche" Unterscheidung zwischen natürlichen und juristischen Personen aufzugeben und beiden gleichermaßen den Informationszugang zu gewähren.

Von den Beschwerden betrafen nahezu die Hälfte den **kommunalen Bereich**, etwa 20 % die Landesbehörden - vor allem die Bezirksregierungen - und nur wenige die Obersten Landesbehörden. Etwa 30 % der Vorgänge betraf unterschiedliche öffentliche Stellen, wie Industrie- und Handelskammern, Landesversicherungsanstalten, Ärztekammern und dergleichen.

Das Schwergewicht im kommunalen Bereich lag erwartungsgemäß bei den **Bau- und Planungsämtern**, wobei die Spanne von der Einsichtnahme in einzelne Bauakten über den gewünschten Zugang zu konkreten öffentlichen Bauprojekten bis hin zur Einsichtnahme in Unterlagen der Bauleitplanung reichte. Auch Liegenschaftsangelegenheiten und Vergabeverfahren interessierten. Bei den Landesbehörden ging es in erster Linie um Ansprüche auf Informationszugang zu Genehmigungs- und Planfeststellungsverfahren, Geschäftsverteilungsplänen, Schulangelegenheiten und Straßenbauprojekten. Bei einer obersten Landesbehörde war der Informationszugang zu Niederschriften über eine Dienstbesprechung mit nachgeordneter Behörden streitig. Ebenfalls wurden Zugangswünsche zu Niederschriften, Prüfungsberichten und Geschäftsordnungen gegenüber verschiedenen juristischen Personen des öffentlichen Rechts geltend gemacht.

Der Anteil der Beschwerden, die sich gegen die Erhebung von **Gebühren** für den gewährten Informationszugang wenden, ist vergleichsweise gering. Dennoch hatten Informationssuchende in einigen Fällen den Eindruck, dass ein erzwungenes Nachgeben auf Seiten der Verwaltung zu einer überhöhten Verwaltungsgebühr geführt habe.

Mit In-Kraft-Treten des Informationsfreiheitsgesetzes haben auch die Zugangsrechte nach dem seit langem geltenden **Umweltinformationsgesetz** und sogar diejenigen nach dem **Datenschutzgesetz Nordrhein-Westfalen** neuen Aufschwung erhalten. Im Bewusstsein der Bürgerinnen und Bürger

ist der Wunsch nach informationeller Teilhabe an den bei den öffentlichen Stellen vorhandenen Informationen offensichtlich gestiegen.

22.2 Streit um die Gesetzesanwendung

Bei Ablehnung von Informationszugangsanträgen werden oftmals Gründe genannt, die weder vom Gesetz gedeckt noch aus Sinn und Zweck des Gesetzes herzuleiten wären. Nicht selten entspringen sie einer unterschwelligen Abwehrhaltung, so als „gehörten" die vorhandenen Informationen allein der Verwaltung.

Eine Stadtverwaltung verweigerte den Zugang zu Unterlagen, die Aufschluss über die Abwicklung eines Auftrags zur Errichtung eines städtischen Gebäudes oder über den Verkauf eines städtischen Grundstücks geben würden, mit der Begründung, es handele sich nicht um Verwaltungstätigkeit, sondern um „rein" privatrechtliches **fiskalisches Handeln**.

Voraussetzung für die Anwendung des Informationsfreiheitsgesetzes ist eine **Verwaltungstätigkeit**, zu deren Zweck Informationen erlangt worden sind (§ 2 Abs. 1 IFG NRW). Diese Festlegung ist zugegebenermaßen nicht klar genug, wenn das Gesetz an gleicher Stelle bestimmt, dass es auf alle Stellen anzuwenden ist, die „Aufgaben der öffentlichen Verwaltung" wahrnehmen (§ 2 Abs.1 IFG NRW). Demgegenüber findet das Gesetz aber auch auf nicht-öffentliche Stellen Anwendung, soweit sie „öffentlich-rechtliche Aufgaben" erfüllen (§ 2 Abs. 4 IFG NRW). In beiden Fällen kommen unterschiedliche Handlungsformen der Stellen, nicht nur die reine Verwaltungstätigkeit im engeren Sinne, in Betracht. Die gesetzliche Festlegung auf „Verwaltungstätigkeit" soll aber **keine Einschränkung** der möglichen Handlungsformen auf eine bestimmte bewirken.

Verwaltungstätigkeit im Sinne des IFG NRW ist **umfassend** und weit zu verstehen, denn § 2 Abs. 1 IFG NRW stellt nicht auf die Rechtsform der Verwaltungstätigkeit ab. Andernfalls würde der gesetzgeberische Wille, Transparenz der öffentlichen Verwaltung herzustellen, in einigen Bereichen ihres Handelns nicht verwirklicht werden können. Das wäre insbesondere auch dann der Fall, wenn öffentliche Stellen aus Kosten- oder Effizienzgründen auf privatrechtliche Organisations- oder Handlungsformen wechselten (OVG Münster, Beschluss vom 19. Juni 2002 - 21 B 589 02). Der Begriff „Verwaltungstätigkeit" ist nicht per se auf ein Handeln der

Exekutive in den Formen des öffentlichen Rechts beschränkt. Er erstreckt sich vielmehr auf **alle Handlungsformen** einer öffentlichen Stelle in hoheitlicher oder privatrechtlicher Form einschließlich des rein fiskalischen Handelns.

Veräußert etwa eine Stadt ein Grundstück, geschieht dies in privatrechtlicher Form. Der **Verkaufsvorgang** ist dennoch als **Verwaltungstätigkeit** im Sinne des § 2 Abs. 1 IFG NRW anzusehen, weil er als Veräußerung eines Vermögenswertes der Stadt nach § 90 Gemeindeordnung NRW nur zulässig ist, wenn das Grundstück zur Aufgabenerfüllung in absehbarer Zeit nicht mehr benötigt wird.

Fraglich könnte auch sein, wie die Formulierung der Anspruchsregelung selbst gemeint ist, die auf den Zugang zu **amtlichen Informationen** bezogen ist. Auch dieser Begriff darf nicht im engen Sinne ausgelegt werden. Vielmehr sind grundsätzlich **alle** bei öffentlichen Stellen **vorhandenen Informationen** amtlich und damit zugänglich. Ausgenommen sind nur private Unterlagen der Beschäftigten, wie beispielsweise eigene Fachbücher, oder solche Unterlagen, die Bürgerinnen oder Bürger gelegentlich einer Antragstellung eingereicht haben, die aber nicht im Zusammenhang mit der begehrten Amtshandlung stehen.

22.3 Vorrang anderer Rechtsvorschriften über den Zugang zu Informationen

Häufig werden Anträge mit dem Argument abgelehnt, der Informationszugang sei in einem speziellen Gesetz geregelt, deshalb könne § 4 Abs. 1 IFG NRW keine Anwendung finden. Die Voraussetzungen des speziellen Informationsrechts seien aber auch nicht gegeben.

Einige Bauämter beispielsweise sehen grundsätzlich den Anspruch auf Informationszugang zu Unterlagen der Bauleitplanung durch die Veröffentlichungsregelungen der §§ 3, 6 und 10 Baugesetzbuch (BauGB) geregelt. Manche Ordnungs- und Genehmigungsbehörden wollen das allgemeine Informationsrecht schon an der Zugangsregelung des § 29 Verwaltungsverfahrensgesetz (VwVfG NRW) scheitern lassen.

§ 4 Abs. 2 IFG NRW ist leider missverständlich formuliert. Bei verständigem Lesen wird aber Folgendes klar: Zunächst sind spezielle Zugangsregelungen zu prüfen. Liegen deren Voraussetzungen nicht vor,

bedeutet dies allerdings noch nicht, dass die vorrangige Regelung in jedem Fall den Rückgriff auf das IFG NRW sperrt. Andernfalls liefe die gesetzgeberische Intention, durch einen **verfahrensunabhängigen Informationsanspruch** die Transparenz des Verwaltungshandelns zu erhöhen, oftmals ins Leere. Im Ergebnis übereinstimmend, in der Formulierung aber deutlicher bringt dies beispielsweise die entsprechende Vorschrift im Berliner Informationsfreiheitsgesetz zum Ausdruck, in der es heißt, dass weitergehende Informationszugangsrechte nach anderen Rechtsvorschriften unberührt bleiben.

Etwa bestehende **Konkurrenzfragen** müssen in jedem konkreten Einzelfall durch eine an Sinn und Zweck der bereichsspezifischen Vorschrift orientierten Auslegung geklärt werden. Dabei gilt, dass ein Vorrang spezieller Zugangsregelungen im Sinne einer verdrängenden Spezialität nur dort bestehen kann, wo die konkurrierenden Normen den selben Lebenssachverhalt regeln, aber zu unterschiedlichen Rechtsfolgen führen.

Wird beispielsweise der Zugang zu Archivmaterial nach Maßgabe des **Archivgesetzes NRW** nur unter engen Voraussetzungen gewährt, so geht es dem IFG NRW vor. Die speziellen Zugangsregelungen zu Archivgut sind nach dem Sinn des Gesetzes abschließend, so dass für denselben Lebenssachverhalt keine unterschiedliche Rechtsfolge eintreten darf. Gerade dieses Beispiel zeigt aber auch, dass noch **gesetzgeberischer Handlungsbedarf** besteht. Solange sich Unterlagen bei der Verwaltung befinden, sind sie nach dem IFG NRW allgemein zugänglich. Wandern dieselben Unterlagen ins Archiv, unterliegt der Zugang zu ihnen plötzlich strengeren Voraussetzungen. Dieses fast als absurd zu bezeichnende Ergebnis sollte mit einer **Harmonisierung** der gesetzlichen Vorschriften vermieden werden.

Wenn dagegen eine bauplanungsrechtliche Vorschrift die öffentliche Bekanntmachung von **Bauleitplänen** vorschreibt, wird damit noch keine besondere Zugangsregelung getroffen, sondern allenfalls eine Veröffentlichungsregelung festgeschrieben. Der allgemeine Informationsanspruch auf Einsichtnahme in Planungsunterlagen eines und einer jeden Informationssuchenden soll damit nicht versperrt sein.

Sehen spezielle Regelungen für bestimmte Personengruppen einen begrenzten Informationszugang vor, so muss geprüft werden, ob diese Grenzen zugleich auch für den allgemeinen Informationsanspruch gelten, um dem Schutzzweck des bereichsspezifischen Gesetzes Rechnung zu

tragen. Nur dort, wo Informationszugangsrechte **bereichsspezifisch abschließend** geregelt sind, muss das IFG NRW zurücktreten.

Wichtigstes Beispiel hierfür ist der immer wieder ins Feld geführte § 29 VwVfG NRW. Danach wird nur den Beteiligten eines laufenden Verfahrens Einsicht in die Unterlagen gewährt, wenn die Kenntnis der Unterlagen zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Die Zugangsregelung des § 29 VwVfG NRW steht der Anwendung des IFG NRW aber nicht entgegen, weil dem Verwaltungsverfahrensgesetz insoweit **keine Sperrwirkung** zukommt. Hierfür spricht die ausdrückliche Einbeziehung des Verwaltungsverfahrens in den Verweigerungsgrund des § 6 Satz 1 Buchstabe b) IFG NRW. Dort hat der Gesetzgeber in Kenntnis des VwVfG NRW die Ablehnung eines Informationszuganges nur im Falle einer erheblichen Beeinträchtigung eines anhängigen Verfahrens zugelassen. Außerdem ist dem Zweck des VwVfG NRW nicht zu entnehmen, dass das engere Zugangsrecht für die Beteiligten notwendig ist, um - über die Verweigerungsgründe nach dem IFG NRW hinaus - die Effektivität der Verwaltung zu sichern.

Auch Kammern und Verbände, die aufgrund eines Bundesgesetzes eingerichtet sind und ein Bundesgesetz ausführen, müssen das IFG NRW für sich akzeptieren. Eine Industrie- und Handelskammer wehrte sich gegen die Anwendung des IFG NRW, weil sie nicht öffentliche Stelle des **Landes** sei, sondern ihre Einrichtung dem (Bundes-)IHK-Gesetz verdanke; die bundesrechtlichen Regelungen aber gingen dem Landesrecht vor. Dieses Argument verkennt, dass die Länder die bundesrechtlichen Regelungen als eigene Angelegenheiten ausführen und gemäß Art. 84 Abs. 1 Grundgesetz unter anderem das Verwaltungsverfahren bestimmen können, soweit im Bundesgesetz nicht etwas anderes festgelegt ist. Das Verwaltungsverfahren umfasst sämtliche Regelungen, die Art und Weise des Verwaltungshandelns betreffen (vgl. VG Düsseldorf Urteil vom 27. August 2002 - 3 K 3073 02).

22.4 Beratung und Begründungspflicht im Verfahren

Die Ablehnungsbescheide sind häufig nicht frei von Fehlern. So werden ohne Nachfrage bei den Informationssuchenden Anträge abgelehnt, weil sie unter dem Kopfbogen einer juristischen Person gestellt werden, an eine falsche Stelle gerichtet sind oder den Informationsgegenstand

nicht ausreichend bezeichnen. Viele Ablehnungen erfolgten weit jenseits der gesetzten Monatsfrist und/oder ohne ausreichende Begründung. Oftmals wurden Anträge auch abgelehnt, weil den Antragstellerinnen oder Antragstellern ein subjektives Interesse an dem Informationszugang vorgehalten wurde.

Die Verfahrensvorschrift des § 5 IFG NRW enthält einige Vorgaben zur Bearbeitung der Informationsanträge, die nur unzureichend verstanden oder beachtet werden. Auch in diesem Verfahren sollte - entsprechend § 25 VwVfG NRW - grundsätzlich Beratung vor Ablehnung gehen. Das bedeutet, dass Informationssuchende darauf hingewiesen werden sollten, dass der Antrag von einer **natürlichen Person** gestellt sein muss, wenn er ihr - wie etwa der Sprecherin oder dem Sprecher einer Bürgerinitiative - nicht schon durch Auslegung zugeordnet werden kann. Auch die Forderung nach **hinreichender Bestimmtheit** wird manchmal überzogen gehandhabt. In Zweifelsfällen würde eine Rückfrage bei den Informationssuchenden dem Selbstverständnis einer bürgerfreundlichen Verwaltung besser entsprechen.

Obwohl in § 5 IFG NRW nicht bestimmt ist, dass die Stelle, bei der die gewünschte Information nicht oder nur vorübergehend vorhanden ist, auf die **richtige Stelle** verweisen muss, ist es für Bürgerinnen und Bürger nicht nachvollziehbar, dass ihre Anträge ohne jegliche Erklärung schlicht abgelehnt werden. Soweit bekannt ist, wo die begehrten Informationen vorhanden sein könnten, sollte auch auf diese Stelle **hingewiesen werden**.

Gravierender sind Verzögerungen von Entscheidungen über die **Monatsfrist** des § 5 Abs. 2 Satz 1 IFG NRW - in vielen Fällen über das Doppelte - hinaus; manchmal wird den Informationssuchenden noch nicht einmal ein Zwischenstand mitgeteilt. Die Frist beginnt mit Eingang des Informationsantrags bei der zuständigen Stelle. Zu einer unkalkulierbaren Verzögerung kann es in der Regel nur kommen, wenn der Informationszugang von einer nach § 10 IFG NRW einzuholenden **Einwilligung** der durch Bekanntgabe betroffenen Person abhängig ist. Deshalb ist vorher immer zu prüfen, ob die Einholung einer Einwilligung nicht dadurch vermieden werden kann, dass die auf die betroffene Person hinweisenden Informationen in den Unterlagen geschwärzt oder sonst **unkenntlich** gemacht werden.

In vielen Fällen wird die **Ablehnung unzureichend begründet**. Meist findet sich nur ein karger Hinweis auf die Gesetzesbestimmung. Die informationssuchende Person muss aber nachvollziehen können, warum der

Informationszugang nicht gewährt werden soll. Immerhin kann es sein, dass der ablehnende Bescheid unzulässig in das Recht auf Information eingreift. Häufig **fehlt** zudem eine Rechtsbehelfsbelehrung, und es unterbleibt trotz § 5 Abs. 2 Satz 4 IFG NRW der Hinweis darauf, dass das Recht besteht, die **Landesbeauftragte** für den Datenschutz als Beauftragte für das Recht auf Information **anzurufen** (§ 13 Abs. 2 IFG NRW). Erfahrungsgemäß wird oftmals erst im Rahmen unserer Prüfung eine ausreichende Begründung seitens der ablehnenden Stelle nachgeliefert.

Dies gilt im Übrigen auch für die Ablehnung der von den Informationssuchenden **gewählten Art** des Informationszugangs (§ 5 Abs. 1 Satz 5 IFG NRW). In vielen Fällen wurde etwa die beantragte Übersendung einer Ablichtung versagt, ohne hierfür eine stichhaltige Begründung anzugeben. Diese Verfahrensweise war **zu beanstanden**.

In anderen Fällen werden Begründungen angeführt, die dem Wortlaut oder der Intention des Gesetzes nicht entsprechen oder sogar zuwiderlaufen. Einem Bürger war der begehrte Informationszugang mit der Begründung versagt worden, er wolle die Informationen nur nutzen, um seine gegen die Stadt erhobene Schadensersatzklage besser begründen zu können. Solche Interessenwahrnehmung sei durch das Informationsfreiheitsgesetz nicht beabsichtigt.

Das Informationsfreiheitsgesetz gewährt aber den **Informationszugang voraussetzungslos** und **unabhängig** von dem dabei **verfolgten Interesse**. Welcher Beweggrund für den Informationszugang besteht, ist völlig unerheblich. Auch kommt es grundsätzlich nicht darauf an, ob der Informationszugang einen rechtlichen oder wirtschaftlichen Vorteil für irgendeine Person schafft. Eine besondere Interessenlage der Informationssuchenden - auch wenn sie von der Verwaltung unerwünscht ist - ist noch kein Ablehnungsgrund (vgl. OVG Münster, Beschluss vom 19. Juni 2002 - 21 B 589/02). Die zulässigen Ablehnungsgründe sind abschließend in § 5 Abs. 4 und §§ 6 bis 9 IFG NRW geregelt. Das verfolgte Interesse ist nur in den seltenen Ausnahmefällen als möglicher Verweigerungsgrund zu berücksichtigen, in denen konkrete Anhaltspunkte dafür bestehen, dass die Informationen zu einer Gefährdung der öffentlichen Sicherheit und Ordnung missbräuchlich verwendet werden sollen (§ 6 Satz 2 IFG NRW).

22.5 Zu den Verweigerungsgründen

In der Gesetzesbegründung wird ausdrücklich klargestellt, dass von einem generellen und **umfassenden Informationszugang** auszugehen ist und die Klauseln mit den Ablehnungsgründen nur als Ausnahmen anzusehen und somit eng auszulegen sind.

22.5.1 Verweigerung des Informationszugangs bei laufenden Verfahren

Manche öffentlichen Stellen nehmen laufende Bauleitplanungs-, Ordnungswidrigkeiten- oder Genehmigungs- und Planfeststellungsverfahren zum Anlass, jeden Antrag auf Informationszugang von vornherein abzulehnen. Verwiesen wird dabei lediglich auf § 6 Satz 1 Buchstabe b) IFG NRW.

Nach § 6 Satz 1 Buchstabe b) IFG NRW ist der Informationszugang aber nur abzulehnen, soweit und solange durch die Bekanntgabe der Information der Verfahrensablauf eines anhängigen Verwaltungsverfahrens **erheblich beeinträchtigt** würde. Ob dies der Fall ist, muss die öffentliche Stelle in jedem Einzelfall prüfen und begründen. Der bloße Hinweis auf die Vorschrift reicht nicht aus.

Selbst wenn eine Verweigerung des Informationszugangs ausnahmsweise zu Recht erfolgt, ist sie allerdings zeitlich begrenzt, solange die Beeinträchtigung des Verfahrenserfolges andauert. Der beantragte Informationszugang ist daher nach **Abschluss des Verfahrens** zu gewähren, sofern keine anderen Verweigerungsgründe greifen.

22.5.2 Schutz des Entscheidungsbildungsprozesses

Entscheidungsfindung und Willensbildung machen den Entscheidungsbildungsprozess nach Maßgabe des § 7 IFG NRW aus. Schwierigkeiten bereitet allerdings schon die Abgrenzung der Informationen, die - unter Berücksichtigung des Grundsatzes der Vollständigkeit der Akte - zu einem bestimmten Vorgang gehören, von jenen Informationen, die unmittelbar zur Entscheidungsfindung führen. Öffentliche Stellen neigen dazu, auf eine solche Abgrenzung zu verzichten und statt dessen den gesamten bisherigen Akteninhalt zum Entscheidungsbildungsprozess zu zählen.

Geschützt nach § 7 Abs. 1 IFG NRW ist allein der Prozess der **Entscheidungsfindung**, um die Effektivität des Verwaltungshandelns zu gewährleisten. Wie der Gesetzeswortlaut zeigt, gehören hierzu nur Entscheidungsentwürfe und unmittelbar vorbereitende Arbeiten wie etwa ein Vermerk zum Entscheidungsentwurf oder interne entscheidungsleitende fachliche Stellungnahmen. Der Schutz umfasst daher nicht das gesamte Informationsmaterial, das einer Entscheidungsfindung dienen kann. Juristische oder sonstige fachliche Stellungnahmen oder Gutachten können in der Regel nicht als entscheidungsvorbereitende Arbeiten angesehen werden, selbst wenn sie für einen konkreten Fall abgegeben oder dafür zur Akte genommen worden sind.

Eine besondere Problematik liegt noch in der Behandlung von **Protokollen über vertrauliche Beratungen**. Da die hierin enthaltenen vertraulichen Informationen auch nach Abschluss des Entscheidungsprozesses unzugänglich bleiben, ist es wichtig, diesen Begriff genauer einzugrenzen, entsprechend der Regel, die Ausnahmeklauseln eng auszulegen.

Der Ablehnungsfall bezieht sich auf ein Protokoll, eine Niederschrift oder auch auf einen Vermerk über vertraulich geführte Besprechungen, bei denen für alle Beteiligten erkennbar Vertraulichkeit vereinbart war. Dies könnte etwa in einer Besprechung mit Investorinnen und Investoren über ein bestimmtes Projekt der Fall sein. Dazu gehören aber nicht schon alle Dienstbesprechungen, die bisher der **Amtsverschwiegenheit** unterlagen. Diese Verpflichtung entfällt im Rahmen der Anwendung des IFG NRW (§ 4 Abs. 2 Satz 2 IFG NRW).

So beharrte ein Ministerium unzulässigerweise darauf, alle Protokolle über Dienstbesprechungen mit nachgeordneten Behörden generell als vertraulich zu behandeln. Vertraulichkeit kann **nicht generell** für Protokolle über **Dienstbesprechungen** erklärt werden; sie kann allenfalls für einen bestimmten Inhalt festgelegt sein und sich auf konkrete behandelte Sachverhalte beziehen.

In ähnlicher Weise verweigerte eine Stadt den Informationszugang zu Rechnungsunterlagen der städtischen Müll- und Abwasserbetriebe mit dem Argument, dass diese Unterlagen als Vorlage für eine nichtöffentliche Sitzung gedient hätten. Auch die **Nichtöffentlichkeit einer Sitzung** reicht allein nicht aus, um alle Informationen, die in einer solchen Sitzung behandelt worden sind, auch inhaltlich als vertraulich zu bezeichnen. Die vertrauliche Behandlung kann nur im engen Sinne verstanden und nur auf

vertrauliche Informationen unmittelbar bezogen werden. Eine andere Auslegung widerspräche dem gesetzgeberischen Ziel, behördliches Handeln für Bürgerinnen und Bürger transparent und nachvollziehbar zu machen.

Eine IHK vertrat die Ansicht, dass ein von beauftragten externen Rechnungsprüfern erstellter Prüfbericht über die Führung der Geschäfte der IHK vertraulich sei. Nur das Ergebnis des Prüfberichtes sei in der Vollversammlung bekannt zu geben. Die Auffassung, der **Prüfbericht** sei auch nach Abschluss der Entscheidung über die Entlastung der Geschäftsführung vertraulich, ist unzutreffend, da im Prüfbericht Informationen enthalten waren, die nach Abschluss des Entscheidungsbildungsprozesses (§ 7 Abs. 3 IFG NRW) grundsätzlich zugänglich gemacht werden müssen. In der Regel dürften bei einer extern durchgeführten Prüfung der Rechnungslegung einer IHK nur objektiv feststellbare Mängel im Prüfbericht auftauchen. Verständlich, aber nicht relevant kann der Wunsch nach Geheimhaltung aufgedeckter Mängel sein. Der Prüfbericht muss daher grundsätzlich zugänglich sein. Selbst wenn einzelne vertrauliche Bewertungen oder Tatsachen in ihm enthalten sein mögen, wird dadurch nicht der ganze Bericht vertraulich. Vielmehr ist der Informationszugang nach eventueller **Schwärzung** der vertraulichen Information zu gewähren.

Nach **Abschluss des Entscheidungsbildungsprozesses** gilt der Verweigerungsgrund nicht mehr, die zurückgehaltenen Informationen sind gemäß § 7 Abs. 3 IFG NRW zugänglich zu machen.

Der **Willensbildungsprozess** ist - neben der oben behandelten Entscheidungsfindung - eigens geschützt. Dieser Schutz bleibt über den Abschluss der Entscheidung hinaus bestehen. Daher ist dieser Ablehnungsgrund gegenüber dem der Entscheidungsfindung noch einmal einzugrenzen.

Ein Bürger wollte Einsicht in die Stellungnahme des kommunalen Umweltamtes zu einer Bauplanänderung nehmen. Den Antrag lehnte das Planungsamt mit der Begründung ab, dass die Stellungnahme verwaltungsintern abgegeben sei und lediglich einen Aspekt der noch nicht abgeschlossenen Willensbildung widerspiegele. Gerade der Dissens innerhalb der Verwaltung interessierte jedoch den Bürger.

Nach § 7 Abs. 2 Buchstabe a) IFG NRW soll der Informationszugang abgelehnt werden, wenn sich der Inhalt der Information auf den Prozess der Willensbildung innerhalb von und zwischen öffentlichen Stellen bezieht. Es

handelt sich um einen Willensbildungsprozess, wenn die Stellungnahme etwa eine streitige Willensbildung erkennen lässt. Der Willensbildungsprozess umfasst **Bewertungen** oder **Einschätzungen**, die intern erst noch beraten werden müssen und unterschiedliche Entscheidungsmöglichkeiten offen lassen. Die Willensbildung spiegelt somit nicht die typische (noch nicht abgeschlossene) Entscheidungssituation aufgrund vorliegender Fakten wieder, sondern eher eine besondere Ausnahmesituation im Vorfeld.

Die Stellungnahme, in die der oben angesprochene Bürger Einsicht begehrte, enthielt eine Wertung, die in der Stadtverwaltung noch nicht abschließend beraten und den kommunalpolischen Gremien noch nicht zur Entscheidung vorgelegt worden war. Die Stadt gewährte dem Informationssuchenden aber den Informationszugang zu der fachlichen Stellungnahme, nachdem sie die vor Veröffentlichung zu schützende **Wertung geschwärzt** hatte.

Nicht alle Unterlagen, die der Vorbereitung einer behördlichen Entscheidung dienen, sind **automatisch Bestandteile** des Bewertungs- und Willensbildungsprozesses. Oftmals stellen sie vielmehr nur eine Voraussetzung für diesen Prozess dar. Eine Verweigerung des Informationszugangs zu diesen Unterlagen kommt allenfalls in Betracht, wenn sonst interne oder zwischen den Behörden ausgetauschte Meinungsäußerungen, Einschätzungen und Bewertungen bekannt würden. Im Falle des Endberichts über ein Förderungsprojekt wird möglicherweise die Aussage zur Fortsetzung der Förderung zu schwärzen sein, es kann aber nicht der ganze Bericht vorenthalten werden.

22.5.3 Schutz von Betriebs- oder Geschäftsgeheimnissen

In der Handhabung der Geheimhaltungspflichten zum Schutz von Betriebs- oder Geschäftsgeheimnissen bestehen große Unsicherheiten. Viele Informationsanträge werden ohne genauere Prüfung vorsorglich abgelehnt, sobald ein solches Geheimnis berührt sein könnte.

Ein **Betriebsgeheimnis** bezieht sich auf Tatsachen, die allein den technischen Betriebsablauf eines Unternehmens betreffen.

Demgegenüber sind Tatsachen, die einem **Geschäftsgeheimnis** unterliegen, schwerer festzustellen. Sie sind zudem abzugrenzen gegenüber dem, was nicht objektiv, sondern nur subjektiv nach dem ausdrücklich oder

konkludent bekundeten Willen einer Unternehmerin oder eines Unternehmers geheim gehalten werden soll. In Zweifelsfällen befragt werden sie immer erklären, dass die begehrten Informationen selbstverständlich dem Geschäftsgeheimnis unterliegen.

Eine Stadt verweigerte beispielsweise die Einsichtnahme in einen Grundstückskaufvertrag mit dem Hinweis auf das Geschäftsgeheimnis des Käufers, der nicht wünsche, dass offenbart werde, zu welchem Kaufpreis und mit welchen Zahlungsbedingungen (wie Ratenzahlung) das Grundstück erworben worden sei.

Dem Geschäftsgeheimnis sind aber nur die Tatsachen unterstellt, die tatsächlich im Zusammenhang mit einem **wirtschaftlichen Geschäftsbetrieb** stehen. Erwirbt beispielsweise ein Unternehmer ein städtisches Grundstück zu einem besonders günstigen Preis, aber für private Zwecke, so kann er keine Geheimhaltung des Kaufpreises verlangen, weil der Kauf nichts mit seinem wirtschaftlichen Geschäftsbetrieb zu tun hat.

Keineswegs sind schon alle vom Willen der Unternehmerin oder des Unternehmers umfassten Angaben - konkludent oder ausdrücklich bekundet - geheim zu halten. Vielmehr muss als weiterer Gesichtspunkt geprüft werden, ob der Gegenstand eines Geschäftsgeheimnisses tatsächlich einem **berechtigten wirtschaftlichen Interesse** entspringt. So können etwa Angaben über Schadensereignisse in einem wirtschaftlichen Geschäftsbetrieb nicht aus berechtigtem Interesse geheim gehalten werden, wenn sie auf Verstößen gegen Unfallverhütungsvorschriften beruhen oder wenn sie unter Verletzung anderer Schutzvorschriften zustande kamen.

Schließlich wäre eine Verweigerung des Informationszugangs nicht gerechtfertigt, wenn dem Geheimhaltungsinteresse des Unternehmens ein **überwiegendes Informationsinteresse der Allgemeinheit** gegenüber stünde (§ 8 Satz 3 IFG NRW). Da das zu schützende Geschäftsgeheimnis, soweit es im Zusammenhang mit der Wahrnehmung öffentlicher Aufgaben steht, meist einer stärkeren Sozial- und Gemeinwohlausrichtung unterliegt als private Geheimnisse, kann die Schutzwürdigkeit gemindert sein. Der Gesetzesvorbehalt in Art. 14 Abs. 1 Satz 2 und Abs. 2 Satz 2 GG ermöglicht nämlich Beschränkungen, die einen Ausgleich mit anderen Rechtsgütern erlauben. Es gibt daher keine grundsätzliche Entscheidung zugunsten des geschützten Geschäftsgeheimnisses. In Fällen, in denen öffentliche Gelder eingesetzt sind oder durch öffentliche Stellen vertragliche Verpflichtungen eingegangen werden, kann unter Berücksichtigung des vom

Informationsfreiheitsgesetzes verfolgten Zweckes - insbesondere der Kontrolle staatlichen Handelns - das Interesse der Allgemeinheit an der Bekanntgabe gerade solcher Daten überwiegen.

Selbst wenn die Einsichtnahme in einen Grundstückskaufvertrag mit dem Hinweis auf das Geschäftsgeheimnis verweigert werden könnte, ist in der Regel von einem Interesse der Allgemeinheit auszugehen. Schon weil solche Veräußerungen von kommunalen Vermögenswerten nur unter bestimmten Voraussetzungen zulässig sind, besteht ein allgemeines Interesse an der Bekanntgabe, das mit dem Geheimhaltungsinteresse des Käufers abgewogen werden muss.

22.5.4 Öffentliche Auftragsvergabe und Informationszugangsrecht

Informationsfreiheit sollte künftig auch zur Bekämpfung von Korruption besser einsetzbar werden.

Wie schon oben unter 22.3 erwähnt, gehen nach § 4 Abs. 2 IFG NRW spezialgesetzliche Zugangsregelungen dem IFG NRW vor. Im Fall der öffentlichen Auftragsvergabe enthält das **Gesetz gegen Wettbewerbsbeschränkungen** (§§ 97 ff. GWB) nicht nur spezielle Zugangsregelungen, die für die Durchführung von Ausschreibungen und Vergabeentscheidungen zwingend vorgeschrieben sind, wenn der Auftragswert die festgelegten Schwellenwerte (§ 2 Vergabeverordnung) überschreitet (für Bauaufträge 5 Millionen € oder für Liefer- und Dienstleistungsaufträge 200.000 €). Die Regelungen des GWB schließen sogar die Anwendung des IFG NRW aus, weil die Geheimhaltung des im GWB geregelten Vergabeverfahrens Vorrang hat. Deswegen haben die Informationsbeauftragten der Länder eine Verbesserung der Informationsfreiheitsgesetze und der Vergabevorschriften empfohlen (vgl. Entschließung der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands zur Korruptionsbekämpfung durch Informationsfreiheit, abgedruckt im Anhang).

Anderes gilt **unterhalb der angegebenen Schwellenwerte.** Hier findet das IFG NRW Anwendung, weil die von den öffentlichen Auftraggebern zu beachtenden Verdingungsordnungen (VOL, VOB) nur als selbstbindende Verwaltungsvorschriften (§ 55 Abs. 2 Landeshaushaltsordnung: einheitliche Richtlinien) und nicht als Rechtsvorschriften im Sinne des § 4 Abs. 2 Satz 1 IFG NRW einzustufen sind. Die Vergabeunterlagen sind demnach zwar

grundsätzlich zugänglich, aber es greifen vielfach die **Verweigerungsgründe** nach §§ 7 und 8 IFG NRW. In diesen Fällen stehen oftmals der Schutz des Entscheidungsbildungsprozesses und der Schutz unternehmensbezogener Daten (Betriebs- oder Geschäftsgeheimnis) einer Offenbarung von Informationen aus dem Vergabeverfahren entgegen.

Deshalb gilt es umso mehr, die noch möglichen allgemeinen Informationszugänge zu öffnen. Vor Abschluss der Ausschreibung ist jedenfalls ein uneingeschränkter Informationszugang zu den Vergabeunterlagen möglich. Nach Eingang der Ausschreibungen wird das Auswahlverfahren in dem **Vergabevermerk** (vgl. § 30 VOB A und VOL A) chronologisch dargestellt. Es werden insbesondere Angaben über die abgegebenen Angebote, die Eignung und Zuverlässigkeit der Bietenden sowie die Wirtschaftlichkeit der Angebote und die Auswahlgründe gemacht. Die Angaben sind personen- oder unternehmensbezogen und daher gemäß §§ 8 und 9 IFG NRW geheim zu halten, soweit mit dem Informationszugang Betriebs- oder Geschäftsgeheimnisse offenbart oder personenbezogene Daten preisgegeben werden. Bedenken bestehen allerdings nicht, wenn der Vergabevermerk ganz oder in Teilen **anonymisiert** zugänglich gemacht wird. Damit wäre die Transparenz und Überprüfbarkeit der im Vergabeverfahren getroffenen Feststellungen und Entscheidungen zumindest ansatzweise möglich. Soweit der Entscheidungsfindungsprozess zur Auftragsvergabe zu schützen ist (§ 7 Abs. 1 IFG NRW), könnte eine Einsicht in den anonymisierten Vergabevermerk nach Zuschlag erfolgen.

22.5.5 Schutz personenbezogener Daten

Nach § 9 IFG NRW ist ein Antrag auf Informationszugang grundsätzlich abzulehnen, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart werden. In der Regel ist somit die Handhabung dieses Verweigerungsgrundes recht einfach. Dies gilt nur dann nicht, wenn einer der gemäß § 9 Abs. 1 Buchstaben a) bis e) IFG NRW ausdrücklich genannten Ausnahmegründe vorliegt.

Die beantragte Einsicht in einen Architektenvertrag, der für eine städtische Baumaßnahme geschlossen worden war, wurde von der Stadt unter Berufung auf den Schutz personenbezogener Daten des Architekten zu Unrecht abgelehnt. Die betreffenden Angaben waren vielmehr **unkenntlich** zu machen und der Informationszugang dann zu gewähren.

Dem Antrag ist nach § 9 Abs. 1 Buchstabe a) IFG NRW zu entsprechen, wenn die von der Offenbarung ihrer Daten betroffene Person eingewilligt hat. Bevor sich die öffentliche Stelle jedoch um eine **Einwilligung** der oder des Betroffenen bemüht, hat sie zunächst zu prüfen, ob ein anderer Ausnahmefall vorliegt oder ob dem Informationsantrag nicht nach **Abtrennung oder Schwärzung** der personenbezogenen Daten stattgegeben werden kann (§ 10 IFG NRW). Erst wenn dies nicht möglich ist, muss sie die Einwilligung der betroffenen Person einholen. Eine Schwärzung allein des Namens reicht allerdings dann nicht aus, wenn bereits durch anderweitige Veröffentlichung der Name des Architekten bekannt ist. Dann müssten weitere Einzelheiten geschwärzt werden.

Wird im Bauamt ein Antrag auf Einsicht in eine bestimmte Bauakte gestellt, kann die Ablehnung dieses Antrags wegen eines möglichen rechtlichen Interesses der informationssuchenden Person unzulässig sein. Im Falle des § 9 Abs. 1 Buchstabe e) IFG NRW gilt nämlich das grundsätzliche Verbot eines allgemeinen Informationszuganges trotz Bekanntwerden personenbezogener Daten nicht. Wenn die Antragsstellerin oder der Antragssteller ein **rechtliches Interesse** an der Kenntnis der begehrten Information geltend macht und keine überwiegenden schutzwürdigen Belange der betroffenen Person entgegen stehen, ist dem Antrag zu entsprechen. Auf eine Einwilligung der betroffenen Person kommt es nicht an. Wird von der informationssuchenden Person hierzu vorgetragen, dass sie prüfen will, ob ihre Rechte beeinträchtigt sind, kann diesem rechtlichen Interesse an der Kenntnis der Information nur entgegen gehalten werden, dass überwiegende schutzwürdige Belange der Bauherrin oder des Bauherrn entgegen stehen.

Wenn beispielsweise die Mieterin oder der Mieter einer Wohnung in einer großen Wohnanlage versucht, durch Einsichtnahme in die entsprechende Bauunterlage die richtige Wohnfläche der von ihr oder ihm gemieteten Wohnung festzustellen und mit der vertraglich vereinbarten Wohnfläche abzugleichen, ist ein entgegenstehender schutzwürdiger Belang nicht erkennbar. Dann reicht eine **Benachrichtigung** der betroffenen Person aus (§ 9 Abs. 2 Satz 1 IFG NRW). Bei der Benachrichtigung ist es nicht erforderlich und damit unzulässig, den Namen der Mieterin oder des Mieters zu nennen. Vielmehr reicht aus, wenn die oder der Betroffene die Mitteilung erhält, dass eine Mietpartei zu dem benannten Zweck Einsicht in die Bauunterlage erhalten hat.

Können durch den Zugang zu einer Information **schutzwürdige Belange der betroffenen Person** beeinträchtigt werden, so hat die öffentliche Stelle ihr vorher Gelegenheit zur **Stellungnahme** zu geben (§ 9 Abs. 2 Satz 2 IFG NRW). Dabei ist zu prüfen, ob der oder dem Betroffenen zur Kenntnis gegeben werden muss, wer die informationssuchende Person ist. Auch für sie gilt der datenschutzrechtliche Grundsatz, dass eine Bekanntgabe nur zulässig ist, wenn die Kenntnis für die oder den Betroffenen erforderlich ist, damit sie ihren oder er seinen schutzwürdigen Belang erkennen kann. Eine Bekanntgabe könnte dann erforderlich sein, wenn die eine Information suchende Person nicht zu dem Personenkreis gehört, der in irgendeiner rechtlichen Beziehung zu der oder dem Betroffenen steht (beispielsweise eine ortsfremde Immobilienmaklerin oder ein -makler ist). Dann sollte die eine Information suchende Person über die Bekanntgabe ihres Namens informiert werden.

Verschiedene Anfragen machen noch einen weiteren Hinweis zum Schutz personenbezogener Daten Dritter in den Fällen beantragter Einsichtnahme unter dem Stichwort **Informantenschutz** notwendig. Akten, wie zum Beispiel der Vorgang eines Ordnungsamtes, enthalten oftmals - möglicherweise sogar unzulässig, weil nicht erforderlich - den Hinweis, wer das Ordnungsamt auf den ordnungswidrigen Zustand aufmerksam gemacht hat. Grundsätzlich darf dies nicht bekannt gegeben werden. Die von der Anzeige betroffene Person selbst hat nur dann einen Anspruch, den Namen der Anzeigeerstatterin oder des -erstatters zu erfahren, wenn sie ein rechtliches Interesse geltend machen kann. Das ist der Fall, wenn die Person, die Anzeige erstattet hat, ihrerseits das Persönlichkeitsrecht der betroffenen Person verletzte, indem sie etwa wider besseres Wissen Unwahres verbreitete (vgl. § 185 Strafgesetzbuch).

Eine weitere **Ausnahmeregelung** vom Verbot des Zuganges zu Informationen mit personenbezogenen Daten findet sich in § 9 Abs. 3 IFG NRW. Danach ist der Schutz der Daten von Amtsträgerinnen und Amtsträgern, Gutachten erstellenden Personen oder Sachverständigen eingeschränkt, sofern sie an dem Vorgang, zu dem der Informationszugang beantragt wird, mitgewirkt oder eine Stellungnahme dazu abgegeben haben.

22.6 Veröffentlichung von Geschäftsverteilungsplänen, Schutz von Beschäftigtendaten

Darf eine öffentliche Stelle ihre Geschäftsverteilungspläne und Organigramme mit Namen, dienstlicher Telefonnummer und E-Mail-Anschrift der Mitarbeiterinnen und Mitarbeiter ohne deren Einwilligung veröffentlichen?

§ 12 IFG NRW sieht die rechtliche Verpflichtung der öffentlichen Stellen vor, ihre bisher üblichen und vorhandenen Geschäftsverteilungspläne, Organigramme und Aktenpläne nach Maßgabe dieses Gesetzes allgemein zugänglich zu machen. § 9 Abs. 3 IFG NRW lässt eine **Offenbarung** von Daten der im **öffentlichen Dienst tätigen Personen** zu. Danach sind Namen (Vor- und Familienname), Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und Rufnummer der Beschäftigten zu veröffentlichen. Unter Büroanschrift ist in Zeiten des Internet (eGovernment) auch - sofern vorhanden - die dienstliche E-Mail-Adresse zu verstehen.

Einer **Einwilligung** der Beschäftigten vor Veröffentlichung ihrer Daten bedarf es **nicht**. Insoweit schränkt das IFG das Recht auf informationelle Selbstbestimmung ein. Im Ausnahmefall können **schutzwürdige Belange** von einzelnen Beschäftigten entgegen stehen. Dann ist die Veröffentlichung der personenbezogener Daten dieser Beschäftigten zu unterlassen. Ein Ausnahmefall kann dann gegeben sein, wenn schwerwiegende Gründe vorgetragen werden, also zum Beispiel eine Gefährdung für Leben oder Gesundheit einer Mitarbeiterin oder eines Mitarbeiters besteht.

22.7 Kosten für den Informationszugang

§ 11 Abs. 1 IFG NRW sieht zwar vor, dass für die Amtshandlungen, die aufgrund dieses Gesetzes vorgenommen werden, Gebühren erhoben werden. Er lässt aber nicht zu, dass bei einer einfachen Akteneinsicht eine Art von „Strafgebühr" erhoben wird. Die Ermöglichung der Akteneinsichtsnahme in einfachen Fällen ist gebührenfrei.

Eine Stadt berechnete für eine mehrmalige - insgesamt zehn Stunden dauernde - Akteneinsicht eine **Gebühr** für die Anwesenheit einer Verwaltungskraft während der Einsichtnahme. Mit einem Stundensatz von 34 € belief sich die Rechnung auf 340 € - eine Summe, die sich die in Existenznot geratene Unternehmerin kaum leisten konnte.

Bei einer Akteneinsicht mit **umfangreichem Verwaltungsaufwand** können Gebühren erhoben werden (§ 1 Verwaltungsgebührenordnung zum IFG NRW, Gebührentarif Nr. 1.3.2). Ein Verwaltungsaufwand kann entstehen bei Arbeiten zur **Vorbereitung einer Akteneinsicht**. Dies kann das Heraussuchen des gewünschten Vorgangs ebenso sein wie die Prüfung des Vorliegens etwaiger Verweigerungsgründe verbunden mit der Einholung einer Stellungnahme oder Einwilligung bei der durch die Informationsgewährung betroffenen Person. Dagegen begründet die **bloße Anwesenheit** einer Verwaltungskraft bei der Akteneinsichtsnahme **nicht** den **Verwaltungsaufwand** im Sinne der Verwaltungsgebührenordnung. Einmal wäre bei ordnungsgemäßer Aktenführung ein unablässiges Beobachten der Person, die die Akteneinsicht begehrt, durch eine Verwaltungskraft nicht erforderlich. Die fortwährende Beobachtung kann sogar den Anspruch auf Informationszugang rechtswidrig beeinträchtigen. Zum Anderen kann die Verwaltungskraft in der Zeit der Einsichtsnahme auch anderen Arbeiten nachgehen. Ist eine Fachkraft zugegen, die auch Fragen beantwortet, muss beachtet werden, dass nach Gebührentarifstelle Nr. 1.1 auch die Erteilung einer mündlichen Auskunft grundsätzlich gebührenfrei ist.

Einer Information suchenden Person, deren **Zahlungsunfähigkeit** bereits bekannt ist, darf der Informationszugang nicht deshalb verweigert werden, weil sie die Verwaltungsgebühren nicht entrichten kann.

Anhang

Entschließungen und andere Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

61. Konferenz am 08./09. März 2001

1. Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung

durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

Alle Neuregelungen wie z.B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

Dem BND wird nicht mehr nur die "strategische Überwachung" des nicht-leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei "strategischen Überwachung" nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

2. Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention).

die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

[1] European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25)

3. Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen,

sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziffer 6.

Entschließungen zwischen den Konferenzen

4. Veröffentlichung von Insolvenzinformationen im Internet (24. April 2001)

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, auf Grund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten

appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 09.03.1988 – 1 BvL 49 86 – zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten. Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

5. Entwurf der Telekommunikations-Überwachungsverordnung (10. Mai 2001)

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße "Surfen" zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.
Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

6. Datenschutzrechtliche Grundanforderungen an die Videoüberwachung in öffentlichen Verkehrsmitteln (05. Oktober 2001)

Die Prüfung der Zulässigkeit von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln richtet sich insbesondere nach § 6 b BDSG. Bei dieser Prüfung sind folgende Gesichtspunkte zu berücksichtigen:

1. Zweck einer Videoüberwachung

Beobachtungen mit Videokameras dürfen im Rahmen der Wahrnehmung des Hausrechts nur zum Schutz vor Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit erfolgen.

Aufzeichnungen werden ausschließlich zum Zwecke der Beweissicherung vorgenommen.

2. Umfang der Beobachtung

Die Videobeobachtung darf nicht der Regelfall sein, sondern nur stattfinden, wenn sie notwendig ist. Es sollte auch geprüft werden, ob den Fahrgästen die Möglichkeit einer unbeobachteten Nutzung des Verkehrsmittels eingeräumt werden kann. Daher verlangt der Einbau von Videokameras in den Verkehrsmitteln eine Einzelfallprüfung mit schriftlichem Vermerk über das Ergebnis; es darf keine automatische Ausstattung aller Verkehrsmittel mit Videokameras stattfinden. Das Erfordernis einer Fortführung der Videoüberwachung ist mindestens alle zwei Jahre festzustellen und zu begründen.

3. Aufzeichnung

Eine Aufzeichnung kann

a) bei einem Vorkommnis im Sinne der Zweckbestimmung für die Dauer des Vorkommnisses veranlasst werden (anlassbezogene Aufzeichnung ohne Historie), oder

b) permanent erfolgen, wird jedoch nach spätestens 20 Minuten automatisch gelöscht, es sei denn, die Löschung wird wegen eines Vorkommnisses im Sinne der Zweckbestimmung verhindert (anlassbezogene Aufzeichnung mit Historie) oder

c) permanent in einem verschlossenen Aufzeichnungsgerät erfolgen, das nur im Falle eines Vorkommnisses (Gewalt gegen Personen oder Beförderungseinrichtungen) von der dazu besonders berechtigten Person geöffnet bzw. ausgelesen wird (anlassungebundene, permanente Aufzeichnung in einer Black Box).

4. Löschung der Aufzeichnung

Bei der anlassungebundenen Aufzeichnung in einer Black Box erfolgt - sofern kein Vorkommnis festgestellt wird - die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich, spätestens nach 48 Stunden. Diese Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung: hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

5. Kreis der berechtigten Personen

Die Beschäftigten, die Zugang zu Aufzeichnungen haben, müssen enumerativ bestimmt werden.

6. Weitergabe von Aufzeichnungen

Es muss festgelegt werden, wer Videoaufzeichnungen weitergeben darf. Es muss außerdem sichergestellt sein, dass die Weitergabe von Videoaufzeichnungen nur zu Beweiszwecken an Polizei, Staatsanwaltschaft oder Gerichte erfolgt.

7. Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder Piktogramme außen und innen die Videoüberwachung kenntlich machen. Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein.

8. Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die benutzten Datenträger, auf denen die Speicherung erfolgen soll, festgelegt werden.

Außerdem muss beschrieben werden, in welchen Fällen ein besonderer Grund vorliegt, d.h. aufgezeichnete Vorkommnisse zur Beweissicherung genutzt werden sollen, dass die beweissichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden müssen sowie die Aufzeichnung zu löschen ist. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

9. Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte ist über geplante Vorhaben zur Einrichtung von Videoüberwachungen rechtzeitig zu unterrichten, da die Vorabkontrolle nach § 4d Abs. 5 BDSG durchzuführen ist. Er trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens „Videoüberwachung" mit den Angaben nach § 4e Satz 1 Ziffern 1 bis 8 BDSG zur Einsichtnahme für Interessenten an geeigneter Stelle bereit liegt.

10. Betriebsvereinbarung

Wegen der möglichen Einbeziehung von Bediensteten in die Videoüberwachung sollte auch eine Betriebsvereinbarung hierüber abgeschlossen werden.

62. Konferenz vom 24. – 26. Oktober 2001

7. 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 bindender 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.

8. 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.

9. 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 Abrechungszwecke 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 personenbezogenen 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.

10. 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 offenlegen, 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.

11. „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.

12. 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 entgegen zu nehmen;
- 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.

63. Konferenz am 07./08. März 2002

13. 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.

14. Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet 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 1.1.2002 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 und Verbindungs- aufzuzeichnen 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.

15. Datenschutzgerechte 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 Internet 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 Internet 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 Internet 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 Internet 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.

16. 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.

Entschließung zwischen den Konferenzen

17. Geplanter Identifikationszwang in der Telekommunikation (24. Mai 2002)

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 bereit gestellt 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.

64. Konferenz am 24./25. Oktober 2002

18. Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit 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.

19. Systematische verdachtslose 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 Telekommunikationsgeheimnisses 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 Mitgliedsstaaten 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 WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig 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.

20. Datenschutzgerechte 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 Internet 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.

Entschließung der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)

Korruptionsbekämpfung durch Informationsfreiheit (20. November 2002)

Die Regierungsparteien haben sich im Koalitionsvertrag darauf verständigt, in der laufenden Legislaturperiode ein Bundesgesetz zur Informationsfreiheit vorzulegen, um das Handeln staatlicher Verwaltung für die Bürgerinnen und Bürger transparenter zu machen. Nachdem die Umsetzung dieses Vorhabens in der vergangenen

Legislaturperiode gescheitert war, begrüßt die AGID den neuen Vorstoß ausdrücklich und erwartet von der Bundesregierung, dass sie mit der Informationsfreiheit nunmehr Ernst macht.

Die aktuellen Korruptions- und Spendenskandale belegen die Notwendigkeit transparenter Strukturen und Verfahren in einem modernen, demokratischen Rechtsstaat. Um das Ziel der Korruptionsbekämpfung zu unterstützen, müssen Informationsfreiheitsgesetze auch bei der für Korruption anfälligen Auftragsvergabe der öffentlichen Hand Wirksamkeit haben. Vergaberechtliche Bestimmungen – insbesondere das Gesetz gegen Wettbewerbsbeschränkungen, die Vergabeverordnung und die Verdingungsordnungen – räumen bislang der Geheimhaltung des Vergabeverfahrens Vorrang ein und behindern die Effizienz bereits bestehender Informationsfreiheitsgesetze der Länder.

Selbst in Fällen, in denen bei Auftragsvergaben unterhalb der festgesetzten Schwellenwerte die landesrechtlichen Informationszugangsregelungen gelten, werden oftmals der Schutz des Entscheidungsprozesses wie auch der Schutz unternehmensbezogener Daten einer Offenbarung von Informationen aus dem Vergabeverfahren entgegengehalten. Eine Kontrolle der den Auftrag vergebenden Stelle durch die Bürgerinnen und Bürger ist somit nicht möglich. Diese überholten Geheimhaltungsvorschriften verhindern transparente Vergabeverfahren.

Deshalb müssen die Informationsfreiheitsgesetze und die Vergabevorschriften dringend so gestaltet werden, dass die öffentliche Auftragsvergabe transparent und für die Allgemeinheit kontrollierbar wird:

Informationsfreiheit muss grundlegender Bestandteil der Vergaberegelungen sein.

Im Hinblick auf das öffentliche Interesse sind die Gründe für die Vergabeentscheidung so weit wie möglich offen zu legen. Unterlagen, die keine Betriebs- oder Geschäftsgeheimnisse enthalten und deren Offenlegung den Entscheidungsprozess nicht beeinträchtigt, zum Beispiel die Niederschrift über die Angebotseröffnung oder die Dokumentation der Auftragsvergabe selbst, sind zugänglich zu machen.

Das öffentliche Interesse an einer transparenten Auftragsvergabe ist gegenüber dem Interesse der bietenden Unternehmen am Schutz ihrer Betriebs- und Geschäftsgeheimnisse stärker zu gewichten.

Stichwortverzeichnis

Abgleichverfahren 149
Abrechnungsdaten 15
Access-Point 42
Ad-hoc-Modus 41
Adresshandel 83
Ahnenrecherche 119
Akteneinsicht 172
Anbieterkennzeichnung 11
Anonymisierung 122
Apotheken, Kundendaten 141
Apotheken-CD 145
Apothekenrechenzentren 141
Arbeitnehmerdatenschutz-
gesetz 99, 105
Archivgut, öffentliches 120
Ärzte, Verordnungsverhalten 134
Auftragsdatenverarbeitung 53
Auskunfteien 77, 93
Auskunftspflicht 170
Auskunftsrecht 82, 89
Auskunftssperre 124
Auskunftsverweigerungsrecht 170
Ausländerzentralregister 148
Authentizität 34, 40
Bedarfsplanung, Kindergarten 128
Begutachtungsverfahren 139
Beihilfedaten, Outsourcing 107
Benachrichtigung 198
Beschäftigte
-E-Mail und Internet 100
-Informationsfreiheitsgesetz 200
-private Post 100
-Vorgesetzte 103
Beschäftigtenkontrolle 7, 100
Beschwerdeausschuss 17
Bestandsdaten 15, 23
Biometrische Merkmale 28, 125
Bluetooth 42
Bodenbelastungsdaten 69
Bonitätsprüfung 71
Bundesstatistik 175
Bundeszentralregister 154
Bürgerbüro 10
Call-Center, Gesundheit 133
CD-ROM-Verzeichnisse 18
Chats 23
Computerkriminalität 14
Corporate Network 12
CRM 7
Cyber Crime Convention 14
Data-Mining-Anwendungen 7
Datenschutzbeauftragte
-behördliche 178
-betriebliche 178
-externe 178
Datenschutzniveau 14, 51
Datensparsamkeit 21, 49
Datenübermittlungsklausel 75
Datenverarbeitungssysteme 10
Datenverarbeitungsvorgänge 49
Datenverkehr, internationaler 51
Datenvermeidung 21, 49
Denkmalliste 68
Deutscher Presserat 17
Direkterhebung 49
DNA-Analyse 162
Durchsuchungsbeschluss 173
Düsseldorfer Kreis 89, 91
eCommerce-Richtlinie 8
eGovernment 10
Einsichtsrecht 139
Einwilligung 7, 87, 110, 116, 162

E-Mail-Werbung 19
Fernmeldegeheimnis 14
Foren 23
Formulare, elektronische 21
FTP-Server 46
Funk-LAN 41
Funkübertragung 40
Geldwäschegesetz 77, 97
genetischer Code 122
Geobasisdaten 64
Gerätekennung 16
Geschäftsgeheimnisse 90
Geschäftszwecke, eigene 86
Gesichtserkennungssysteme 58
Gesundheitsdaten 107, 118
Gesundheitsdatenschutzgesetz 139
Gewaltenteilung, informationelle 11
GSM 40
Hausrecht 56
Homepage 11
Identifizierung 78
IMSI-Catcher 4, 16
Informationen, amtliche 186
Informationsfreiheitsgesetz 2, 113, 130, 183, 184, 185, 187, 190, 196
Informationspflichten 8
Infrastruktur-Modus 41
Inhaltsdaten 21
INPOL-BKA 154
Insolvenzverfahren 167
Integrität 34, 40
Internetdateien, temporäre 22
Internetpranger 95
Konvergenz der Medien 9
Korruptionsbekämpfung 196
Krankenhausentlassungsberichte 141
Kriminalakten 153
Kundenbewertung 7
Kundenbindungsprogramme 76, 85
Kundenkarte 86, 142
Lastschriftverfahren 84
Legitimationsvermerk 88
Luftbildaufnahme 66
Mailing-Listen 20
medizinischer Dienst 141
Medizinnetze 31
Melderegisterauskünfte 124
MESTA 160
Mietbewerbungsbogen 62
Miles & More 75
Mobilfunkkarten 16
molekulargenetische Untersuchung 162
Nebenstellenanlagen 13
Negativmerkmale
-harte 95
-objektive 61
Netzkennung 16
Netzwerkmanagementtools 104
Newsgroups 23
Newsletter 20
Nicht-Abstreitbarkeit 31, 37, 38
Nutzung, anonyme 23
Nutzungsdaten 15, 24
Nutzungsfestlegung 39
Nutzungsprofile 8
Öffentlichkeitsfahndung 160
Ordnungspartnerschaft 156
P3P 43
Passwortspeicherung 22
Patientenbücher 140
Personalaktendaten 108, 117
Personalausweisdaten 77
Personalausweislesegeräte 165
Personalausweisnummer 78
Personalrat 109
Personenstandsbücher 119

Persönlichkeitsrecht 57
Plausibilitätsprüfungen 45
Pressekodex 17
Privatpost 99
Prognoseentscheidung 163
Protokolldateien 104
Protokolle über Dienstbesprechungen 192
Pseudonymisierung 122
Quittungsverfahren 102
Rasterfahndung 5. 151. 153
Rats- und Ausschusssitzungen 126
Redaktionsdatenschutz 17
Revisionsfähigkeit 36
Revisionssicherheit 10
richterliche Anordnung 162
Richtervorbehalt 163
Risikoanalyse 32
Rückwärtssuche 18
Safe Harbor Abkommen 53
SCHUFA 78. 91. 93
Schuldnerverzeichnis, zentrales 167
Schweigepflichtentbindungserklärung 135
Scoringverfahren 91
Selbstauskunft 62. 78. 92
Selbstkontrolle, publizistische 17
Sicherheitsdienste, private 156
Sicherheitsvorgaben 12
Sicherungsinfrastruktur 9
Signatur
-elektronische 9. 34
-qualifizierte 37
Sozialdaten
-Akteneinsichtsrecht 130
-Formulare 132
-Informationsfreiheitsgesetz 130
-Rasterfahndung 151
Spammails 19
Sperrung 93
Spionageprogramme 104
Standardvertragsklauseln 53
Systemadministration 104
Teledienste 8. 21
Telefax 47
Telefonüberwachungen 4
Telefonverzeichnisse 18
Telekommunikation 18
Telekommunikationsgeheimnis 6. 101
Terrorismusbekämpfungsgesetz 3. 148. 150
Trojanische Pferde 22
Trustcenter 9
UMTS 40
unerwünschte Werbung 83
Unterlagenvernichtung 48
Unternehmensregelungen 54
Unterrichtungspflicht 11. 49. 83
Validität 37
Verbindungsdaten 14
Verbot mit Erlaubnisvorbehalt 49
Verbraucherorganisation 80
Verbunddateien 155
verdachtslose Speicherung 6
Verfahren, Defintion 179
Verfahrensdaten 160
Verfahrensverzeichnis 179
Verfügbarkeit 35
Verifikation 28
Veröffentlichungsbefugnis 79
Verschlüsselung 11. 21. 33. 34. 41. 43
Verschwiegenheitspflicht 170
Versichertendaten 133
Vertraulichkeit 21. 33. 40
Verwaltungsaufwand 201
Verwaltungstätigkeit 185
Videoüberwachung 50. 55
Virenscanprogramme 101

virtuelles Datenschutzbüro 28
VNC 25
Volljährigkeitsregelung 116
Vorabkontrolle 179
Wahlverhalten 7
Warndatei 6, 60, 94
Warnhinweise 80
Webcams 55
WEP 41
Werbe-Sperrdatei 82
Werbezwecke 81, 111
Wettbewerb, unlauterer 19
Widerspruch 92, 124
Widerspruchsrecht 50, 82
Willensbildungsprozess 193
Willenserklärungen 9
Wireless-LAN 41
Zahlungsverkehr, bargeldlos 84
Zertifizierungsstellen 9
Zugriffsberechtigung 102
Zweckbindung 50

Datum: .....

Absender in:

.....

(Vorname, Name)

.....

(Behörde)

.....

(Straße, Hausnummer Postfach)

.....

(PLZ, Ort)

Landesbeauftragte
für den Datenschutz und Beauftragte
für das Recht auf Information
Nordrhein-Westfalen
Reichsstraße 43

40217 Düsseldorf

Betr.: Informationsmaterial

Hiermit bitte ich um Übersendung folgender Broschüren:

_____ Aufkleber zum Adressenhandel

_____ Datenscheckheft

_____ Datenschutz in der Europäischen Union

_____ Datenschutzrecht des Landes NRW

_____ den neuesten Datenschutzbericht

_____ den ..... Datenschutzbericht

_____ 20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?

_____ Datenschutzgerechtes eGovernment

_____ Faltblatt Datenschutz ... ist Ihnen egal?

_____ Faltblatt Adresshandel und unerwünschte Werbung

_____ Faltblatt Datenschutz im Verein

_____ Faltblatt Handels- und Wirtschaftsauskunfteien

_____ Handys - Komfort nicht ohne Risiko

_____ Orientierungshilfe Behördliche Datenschutzbeauftragte

_____ Orientierungshilfe Schulen ans Netz

_____ Orientierungshilfe Archivierung von Krankenunterlagen-Outsourcing

_____ Orientierungshilfe Datenschutz im Personalrat

_____ Orientierungshilfe Datenschutz und Datensicherheit beim Betrieb von IT-Systemen

_____ Orientierungshilfe Telefax

_____ Orientierungshilfe Unterlagenvernichtung

_____ Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

_____ Serviceorientierte Verwaltung „Vom Bürgerbüro zum Internet"

Mit freundlichen Grüßen

Notizen

NRW.

http://www.lfd.nrw.de